Technická univerzita v Liberci
FAKULTA PEDAGOGICKÁ

Katedra: Matematiky a didaktiky matematiky
Studijní program: Učitelství pro 3. stupeň
Kombinace: matematika, zeměpis

Základy teorie grup
Elements of Group Theory

Diplomová práce: 08–FP–KMD–005

Autor:
Milan KALIŠ

Podpis:

Adresa:
Riegrova 289
463 42, Hodkovice nad Mohelkou

Vedoucí práce: Doc. RNDr. Jaroslav VILD
Konzultant:

Počet

stran	slov	obrázků	tabulek	pramenů	příloh
69	17849	12	31	16	0

V Liberci dne:

(zadání)

Prohlášení

Byl(a) jsem seznámen(a) s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

V Liberci dne: Milan Kališ

_____

ZÁKLADNÍ PRVKY TEORIE GRUP

KALIŠ Milan **DP– 08 -FP-KMD - 005** **Vedoucí DP:** Doc. RNDr. Jaroslav Vild

Anotace

V diplomové práci jsou zpracovány základní pojmy a oblasti studia teorie grup. Jde především o konečné grupy, jejich strukturu a vlastnosti. Speciální ohled je věnován podgrupám, cyklickým grupám, zvláště grupě $\mathbb{Z}_n$. Práce zahrnuje nejen základní definice a věty, ale i spoustu příkladů, řešených příkladů, tabulek a grafických příloh. V závěru je shrnuto využití teorie grup v matematice a jiných oblastech života.

Elements of Group Theory

Summary

This Diploma thesis is processing fundamental principles and areas of Group Theory. Primary focus is on finite groups, its structure and properties. Special attention is payed to subgroups, cyclic groups and the group $\mathbb{Z}_n$. This work covers not only fundamental definitions and theorems, but also a lot of examples, solved problems, tables and graphical appendices. In final chapter is covered usage of the Group Theory in mathematics and other areas of life.

Poděkování

Chtěl bych poděkovat panu Doc. RNDr. Jaroslavu Vildovi za jeho vedení, podporu, poskytnutí důležitých podkladů a podnětných nápadů, které mě inspirovaly a usnadnily tak tvorbu této diplomové práce. Dále bych chtěl poděkovat i své rodině za psychickou i materiální podporu.

Obsah

Seznam užitých symbolů, značek a grafických úprav

$\mathbb{N}$	množina všech přirozených čísel: {1, 2, 3, 4, 5, …}
$\mathbb{N}_k$	množina úvodních k přirozených čísel ({1, 2, 3, 4, 5, …, k}, kde $k \in \mathbb{N}$)
$\mathbb{Z}$	množina celých čísel
$n\mathbb{Z}$	množina $\{n \cdot k;\ k \in \mathbb{Z}\}$ pro dané přirozené číslo n; množina všech celočíselných násobků přirozeného čísla n
$\mathbb{Z}_n$	n-prvková množina zbytkových tříd modulo n
$\mathbb{Q}$	množina všech racionálních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{Q}^+$, $\mathbb{Q}^-$	množina všech kladných, množina záporných racionálních čísel
$[x, y]$	uspořádaná dvojice čísel x, y (kde x, y patří do nějaké množiny $\boldsymbol{A}$)
$\boldsymbol{GL}_n(\mathbb{R})$	množina všech regulárních matic typu $n \times n$ s prvky z tělesa $\mathbb{R}$
$\emptyset$	označení pro prázdnou množinu
$a \in \boldsymbol{A}$	prvek a patří do množiny $\boldsymbol{A}$
$\boldsymbol{A} \subset \boldsymbol{B}$	množina $\boldsymbol{A}$ je podmnožinou množiny $\boldsymbol{B}$
$\boldsymbol{A} \setminus \boldsymbol{B}$	(množinový) rozdíl množin $\boldsymbol{A}$, $\boldsymbol{B}$ (v tomto pořadí)
$\boldsymbol{A} \times \boldsymbol{B}$	kartézský součin množin $\boldsymbol{A}$ a $\boldsymbol{B}$; množina všech uspořádaných dvojic $[a, b]$ všech prvků $a \in \boldsymbol{A}$, $b \in \boldsymbol{B}$
$f : \boldsymbol{A} \to \boldsymbol{B}$	zobrazení f, které prvkům množiny $\boldsymbol{A}$ přiřazuje prvky množiny $\boldsymbol{B}$
$a \mid b$	prvek a dělí prvek b (kde $a, b \in \mathbb{Z}, a \neq 0$)
$\boldsymbol{A} \wedge \boldsymbol{B}$	konjunkce výroků $\boldsymbol{A}$ a $\boldsymbol{B}$ [čteme: $\boldsymbol{A}$ platí a (zároveň) $\boldsymbol{B}$ platí]
$\boldsymbol{A} \vee \boldsymbol{B}$	disjunkce výroků $\boldsymbol{A}$ a $\boldsymbol{B}$ [čteme: $\boldsymbol{A}$ platí (a)nebo $\boldsymbol{B}$ platí]
$\boldsymbol{A} \Rightarrow \boldsymbol{B}$	implikace výroků $\boldsymbol{A}$ a $\boldsymbol{B}$ [čteme: jestliže platí výrok $\boldsymbol{A}$, platí i výrok $\boldsymbol{B}$]
$\boldsymbol{A} \Leftrightarrow \boldsymbol{B}$	ekvivalence výroků $\boldsymbol{A}$ a $\boldsymbol{B}$ [čteme: $\boldsymbol{A}$ platí, právě když $\boldsymbol{B}$ platí]
$\neg \boldsymbol{A}$	negace výroku $\boldsymbol{A}$ [čteme: neplatí $\boldsymbol{A}$; není pravda, že platí $\boldsymbol{A}$]

$o(a)$	řád prvku a dané grupy; nejmenší přirozené číslo k, pro které platí $a^k = e$, kde e je neutrální prvek grupy dané operace
$\lvert \mathbf{G} \rvert$	řád grupy **G**
$\lvert \boldsymbol{M} \rvert$	počet prvků (konečné) množiny $\boldsymbol{M}$
$\langle a \rangle$	cyklická grupa generovaná svým prvkem a
$\boldsymbol{M}/\boldsymbol{R}$	rozklad množiny $\boldsymbol{M}$ podle ekvivalenční relace $\boldsymbol{R}$
$\mathbf{G}/\mathbf{H}$	rozklad grupy **G** podle podgrupy **H** na levé (pravé) třídy
$[\mathbf{G} : \mathbf{H}]$	index podgrupy **H** v grupě **G**; počet všech různých levých tříd grupy **G** podle podgrupy **H**
$\mathbf{H} \leq \mathbf{G}$	grupa **H** je podgrupou grupy **G**
$\mathbf{G} \simeq \mathbf{H}$	grupa **G** je isomorfní s grupou **H**
$[a]$	třída rozkladu reprezentovaná prvkem a
$\equiv_n$	rovnost modulo n, kde n je číslo přirozené
$+_n$	sčítání modulo n, pro přirozená čísla n
[,]	závorky pro komentář
Def.	zkratka pro definici
Pozn.:	zkratka pro poznámku; všechny poznámky jsou podšeděny
◄, ►	označení začátku, konce důkazu

1. Úvod

Teorie grup je disciplína abstraktní algebry. Specializuje se na studium specifických algebraických struktur, grup. Tato disciplína vznikla ze tří hlavních matematických oblastí: geometrie počátku 19. století; teorie čísel konce 18. století a teorie algebraických rovnic, která vedla ke studiu permutací. Samozřejmě řada pojmů a vět, které teorie používá, pochází z doby mnohem starší.

Na přelomu 18. a 19. století se do popředí studia geometrie dostávala *n*-rozměrná geometrie, což je záležitost abstraktní. Studie některých matematiků vedly k třídění geometrií, což byla určitá analogie později zavedeného pojmu isomorfie, který je samozřejmě zahrnut i v tomto textu.

V polovině 18. století se o významné výsledky zasloužil matematik L. Euler při studiu modulární aritmetiky, zbytků po dělení mocnin modulo *n*. Euler už v té době intuitivně pracoval s cyklickými grupami a jejich rozklady podle podgrupy. Na jeho práci navázal další veliký matematik K. F. Gauss, který výsledky Eulerových studií posunul mnohem dále. Gauss studoval především abelovské grupy a došel k mnoha závěrům, týkajícím se řádu prvků. Eulerův současník J.-L. Lagrange studoval vlastnosti permutací při hledání řešení bikvadratických a kubických algebraických rovnic. Přestože Lagrange sám nedošel k pojmu podobnému grupě, jeho zásluhy pro pozdější teorii grup permutací a grup symetrických jsou značné.

Až v roce 1799 italský matematik P. Ruffini zavedl pojem grupa permutací v práci, zabývající se důkazem neřešitelnosti algebraické rovnice pátého řádu. Ruffini dělil grupy permutací do určitých tříd, které se v dnešní době označují za grupy cyklické. S dalšími významnými výsledky přišli v polovině 19. století matematici A. L. Cauchy a N. H. Abel.

Jejich současník E. Galois byl prvním, kdo porozuměl grupám permutací a plně jich využíval při řešení problémů, týkajících se algebraických rovnic. Studoval nejen podgrupy grup permutací, ale i rozklady grup permutací podle těchto podgrup. V pozdější době se teorie grup obohatila o pojem isomorfie grup, který zavedl další významný matematik M. E. C. Jordan. F. Ch. Klein se v této době postaral o další výsledky teorie grup v oblasti geometrie. Ve své práci se pokusil o grupově teoretickou klasifikaci geometrie, což posunulo teorii grup do popředí matematického zájmu.

V polovině 19. století se o obrovský „boom“ zasloužil v teorii grup velice významný matematik A. Cayley, který zavedl pojem abstraktní grupa. Ukázal tedy, že neexistují pouze grupy permutací (což byly v podstatě jediné grupy, které se dosud studovaly), ale i jiné grupy. Cayley byl zároveň autorem multiplikačních tabulek operací grup, které jsou používány dodnes.

Na přelomu 19. a 20. století byly napsány základní soubory prací, zahrnující významné výsledky

teorie grup. V neposlední řadě tedy zmiňme i „novodobější“ významné matematiky F. G. Frobenius, L. Kronecker, W. Burnside nebo J. W. R. Dedekind, kteří předali štafetu matematikům 20. století.

Cílem této práce je zpracovat obsah základů teorie grup tak, aby byla dobře čitelná a dobře pochopitelná pro cílovou skupinu studentů nižších ročníků fakult vysokých škol (především budoucích studentů učitelství). Dále se snažím vyřešit nedostatky, se kterými jsem se sám během svého studia matematických knih setkal. Pro přehlednost udávám na začátku každé kapitoly klíčové pojmy, které budou v dané kapitole uvedeny a vysvětleny. Příklady, způsoby zápisu definic a vět volím podle své zkušenosti se svými kolegy (studenty pedagogické fakulty), ale zároveň přitom zachovávám základní konvence formy matematických publikací. Na konci každé kapitoly a v textu uvádím reference, ze kterých jsem na příslušné téma čerpal. Označuji je zkratkou v hranatých závorkách a jejich citace je v kapitole Seznam užitých pramenů.

V textu jsou i obrázky, tabulky a příklady, které slouží jako nástroj lepší názornosti a pro přehlednost. Jejich značení jsem zvolil ve tvaru: *typ.kapitola.číslo* (tedy např. Obr. 3.2 je druhý obrázek ve třetí kapitole). Dále jsem přidal i několik řešených příkladů, které osvětlují postupy při řešení některých typů úloh.

V kapitole Algebraické struktury jsou shrnuty základní pojmy, se kterými se čtenář bude dále setkávat. Jedná se především o pojmy pomocné, které jsou třeba v definicích pojmů teorie grup. Další kapitola Konečné grupy zahrnuje definici a významné vlastnosti grup. Kapitola podgrupy a cyklické grupy pojednává o podstrukturách grup a jejich prvcích. Následujícím tématem je ekvivalence prvků grupy v kapitole Rozklad grupy. Tato část textu se přes ekvivalenci, rozklad grupy podle podgrupy a index podgrupy v grupě dostává až k významné Lagrangeově větě, jejíž důsledky jsou zde také vysvětleny. Ve dvou kapitolách Isomorfismus a Klasifikace grup se čtenář dozví, jakým způsobem můžeme grupy porovnávat a poté třídit do „skupin“. Navíc jsou zde popsány základní druhy grup, se kterými se matematik setkává. V předposlední kapitole je osvětlena teorie, týkající se reprezentací grup grupami permutací. Poslední kapitola zahrnuje shrnutí a využití teorie grup v praxi.

Mým záměrem bylo zpracovat tématiku teorie grup novým způsobem tak, abych vyplnil co nejvíce mezer, se kterými jsem se setkal při studiu ostatních textů, ze kterých jsem čerpal. Především jsem se zaměřil na vhodné příklady a podrobnější provádění důkazů vět. Dále jsem text strukturoval podle návaznosti pojmů, které jsem minimalizoval. Čerpal jsem především z anglicky psané literatury, takže většina textu je interpretována mnou samým, což by se mělo projevit v jednotnosti textu a jeho originalitě.

Reference: [**OCR**].

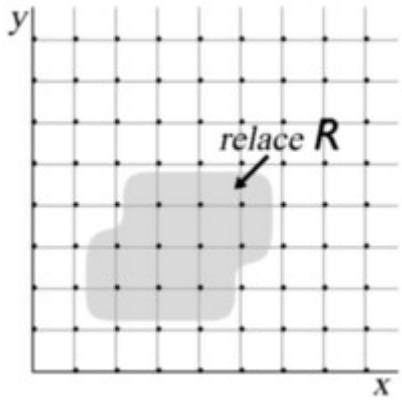
2. Algebraické struktury

Relace, zobrazení, binární operace, celočíselná mocnina prvku, algebraická struktura.

V tomto textu předpokládám, že čtenář je úspěšný absolvent střední školy, takže nebudu vysvětlovat pojmy, týkající se teorie množin a klasické logiky. Pro komplexnost této práce však uvedu několik důležitých pojmů, se kterými se bude čtenář dále často setkávat.

Def. (Relace na množině): Libovolnou podmnožinu $\boldsymbol{R}$ kartézského součinu množiny $\boldsymbol{M}\times\boldsymbol{M}$, kde $\boldsymbol{M}\neq\emptyset$), nazveme (binární) *relací na množině* $\boldsymbol{M}$. Prvky $a,b\in\boldsymbol{M}$, které jsou v relaci $\boldsymbol{R}$ zapisujeme $a\boldsymbol{R}b$, nebo $[a,b]\in\boldsymbol{R}$.

Obr. 2.1. Grafické znázornění vybrané relace $\boldsymbol{R}$



(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Kartézský součin $\boldsymbol{M}\times\boldsymbol{M}$ prvků $x,y\in\boldsymbol{M}$ se dá graficky znázornit jako síť bodů. Libovolná podmnožina $\boldsymbol{R}$ těchto bodů se nazývá relace (vyznačeno v obrázku šedým podkladem).

Def. (Vlastnosti relace): Mějme relaci $\boldsymbol{R}\subset\boldsymbol{M}\times\boldsymbol{M}$. Pak $\boldsymbol{R}$ nazveme

1) *reflexívní*, pokud $\forall a\in\boldsymbol{M}; a\,\boldsymbol{R}\,a$ [tedy každý prvek a je v relaci $\boldsymbol{R}$ se sebou samým; například u relace rovnosti],

2) *symetrická*, pokud $\forall a,b\in\boldsymbol{M}; a\,\boldsymbol{R}\,b\Rightarrow b\,\boldsymbol{R}\,a$ [pokud je prvek a v relaci $\boldsymbol{R}$ s prvkem b, je i prvek b v relaci $\boldsymbol{R}$ s prvkem a],

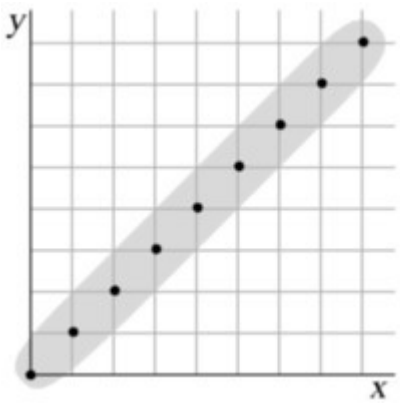
3) *antisymetrická*, pokud platí $\forall a,b\in\boldsymbol{M}; a\,\boldsymbol{R}\,b\wedge b\,\boldsymbol{R}\,a\Rightarrow a=b$ [pokud je prvek a v relaci $\boldsymbol{R}$ s prvkem b a i prvek b je v relaci $\boldsymbol{R}$ s prvkem a, musí si být tyto prvky rovny],

4) *tranzitivní*, pokud $\forall a,b,c\in\boldsymbol{M}; a\,\boldsymbol{R}\,b\wedge b\,\boldsymbol{R}\,c\Rightarrow a\,\boldsymbol{R}\,c$ [pokud je prvek a v relaci $\boldsymbol{R}$ s prvkem b a zároveň prvek b je v té samé relaci s prvkem c, je i prvek a v relaci $\boldsymbol{R}$ s prvkem c].

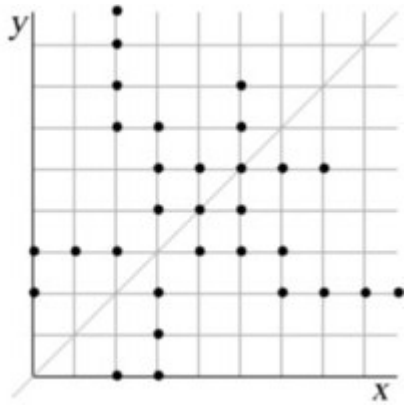
Pozn.: Vlastnost symetričnost není splněna například u relace „<“.

Příklad 2.1.: Rovnost je jedna z tzv. ekvivalenčních relací, které splňují vlastnosti 1), 2), 4) výše. Relace „být větší nebo rovno“ ≥ je reflexívní, tranzitivní, antisymetrická, není tedy ekvivalencí.

Obr.2.2a Vlastnosti reflexívní relace



Obr.2.2b Vlastnosti symetrické relace



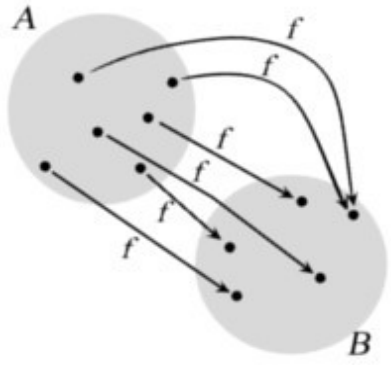
(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Obrázek obr.2.2a znázorňuje hlavní grafický projev reflexívnosti relace. Tedy pokud je relace reflexívní, musí obsahovat všechny body sítě, které jsou na diagonále (na obrázku znázorněno podšeděním). (Kromě bodů na diagonále může reflexívní relace obsahovat i další body sítě.)

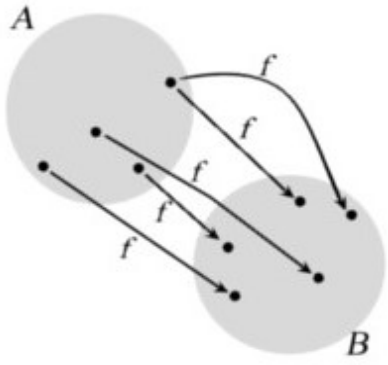
Hlavním grafickým projevem symetrické relace je, že všechny uspořádané dvojice kartézského součinu $\boldsymbol{M}\times\boldsymbol{M}$, které jsou na obrázku obr.2.2b interpretovány jako body, jsou osově symetrické podle diagonály (která je znázorněna šedou barvou).

Def. (Zobrazení): Mějme dvě neprázdné množiny ***A***, ***B***. Relaci *f*, která každému prvku $x\in\boldsymbol{A}$ přiřazuje nejvýše jeden prvek $y\in\boldsymbol{B}$ tak, že uspořádaná dvojice $[x, y]\in f$, nazveme *zobrazení množiny **A** do množiny **B***. Prvek *x* nazýváme *vzorem* prvku *y* v zobrazení *f*. Prvek *y* nazýváme *obrazem* (nebo hodnotou) prvku *x* v zobrazení *f*; často se značí *f*(*x*).

Obr.2.3a Ukázka relace zobrazení



Obr.2.3b Ukázka relace, která není zobrazením



(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Na obrázcích jsou šedou barvou znázorněny dvě neprázdné množiny ***A***, ***B***; jejich prvky jsou znázorněny body. Pravidla zobrazení *f* z množiny ***A*** do množiny ***B*** jsou znázorněna pomocí šipek. V obrázku Obr.2.3a jsou splněny podmínky definice zobrazení. Obrázek Obr.2.3b není znázorněním relace zobrazení, jelikož jednomu bodu množiny ***A*** jsou přiřazeny dva body množiny ***B***.

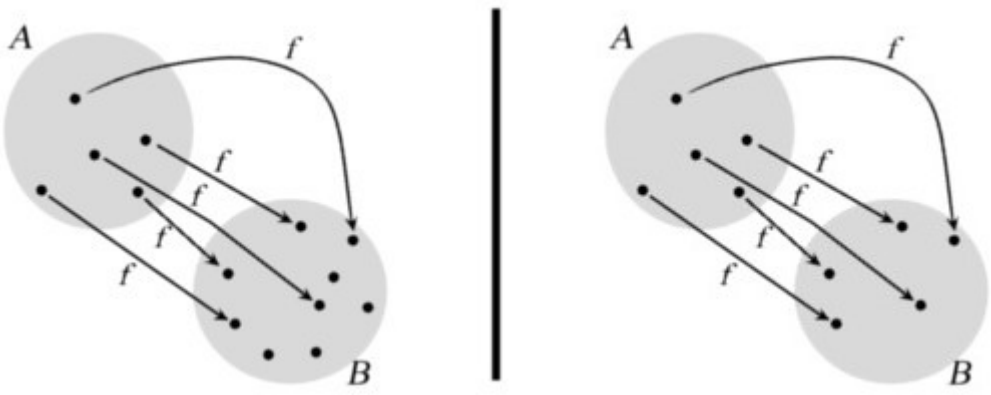
Def. (Prosté (injektivní) zobrazení): Zobrazení množiny ***A*** do množiny ***B*** nazveme *prostým* (injektivním) *zobrazením*, právě když každým dvěma různým vzorům $x_1, x_2 \in \boldsymbol{A}$ odpovídají dva různé obrazy $f(x_1), f(x_2) \in \boldsymbol{A}$.

Def. (Surjektivní zobrazení): Prosté zobrazení $f : \boldsymbol{A} \rightarrow \boldsymbol{B}$, u kterého obrazy všech prvků množiny ***A*** pokryjí celou množinu ***B***, nazveme s*urjektivní* (zobrazení na).

Def. (Bijektivní zobrazení): Prosté surjektivní zobrazení nazýváme *bijektivní zobrazení*.

Obr.2.4. a) Ukázka prostého zobrazení

Obr.2.4. b) Ukázka bijektivního zobrazení



(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Prosté zobrazení (Obr.2.4a) se vyznačuje tím, že do každého bodu množiny ***B*** vede nejvýše jedna šipka z bodu množiny ***A*** (tedy každý bod z obrazové množiny ***B*** má nejvýše jeden vzor). Obrázek obr.2.3a ukazuje zobrazení, které není prosté. Bijektivní zobrazení (Obr.2.4b) je charakteristické tím, že každý bod množiny ***A*** má právě jeden obraz v množině ***B***, a zároveň každý bod z obrazové množiny ***B*** má právě jeden vzor.

Příklad 2.2.: Zobrazení SEZNAMKA, které každému prvku z množiny ***M*** := {množina 25 nezadaných mužů} přiřadí právě jeden prvek množiny ***Ž*** := {množina 25 nezadaných žen}, je prosté, navíc celá množina ***Ž*** bude mít svůj vzor, tedy SEZNAMKA je bijektivní zobrazení. Pokud by množina ***Ž*** obsahovala 26 prvků, už by se jednalo pouze o prosté zobrazení. Pokud by bylo v zobrazení SEZNAMKA povoleno mnohoženství (tedy jeden prvek z ***M*** by mohl mít vícero obrazů z

množiny $\check{\boldsymbol{Z}}$), byla by SEZNAMKA pouze relace, nikoliv zobrazení.

Dalším důležitým pojmem je operace. Dále v textu budeme používat především operace binární, tedy operace na dvojicích prvků.

Def. (Binární operace): Zobrazení $O : \boldsymbol{M} \times \boldsymbol{M} \to \boldsymbol{M}$ nazýváme *binární operace O* na množině $\boldsymbol{M}$. Prvek *aOb* (kde $a, b, aOb \in \boldsymbol{M}$) nazýváme *kompozicí prvků a*, *b* vzhledem k binární operaci *O*.

Tedy například sčítání přirozených čísel je binární operace $+: \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$, pak např. Prvek 3 + 5 nazýváme kompozice prvků 3, 5 vzhledem k operaci sčítání „+“. Zobrazení SEZNAMKA: $\boldsymbol{M} \to \check{\boldsymbol{Z}}$ není binární operace (jedná se o tzv. unární operaci).

Def. (Vlastnosti binárních operací): Mějme operaci $O : \boldsymbol{M} \times \boldsymbol{M} \to \boldsymbol{M}$, libovolné prvky $a, b, c \in \boldsymbol{M}$ a nechť je definována rovnost „=“ prvků z $\boldsymbol{M}$. Operaci *O* na množině $\boldsymbol{M}$ nazveme

a) *asociativní*, pokud $(aOb)Oc = aO(bOc)$ [tedy můžeme tři libovolné prvky uzávorkovat],

b) *komutativní*, pokud $aOb = bOa$ [tedy nezáleží na pořadí operandů],

c) s *neutrálním prvkem* $e \in \boldsymbol{M}$ vzhledem k operaci *O*, pokud $aOe = eOa = a$

[výsledkem kompozice prvku *a* a neutrálního prvku *e* vůči dané operaci je vždy prvek *a*],

d) má-li operace *O* na $\boldsymbol{M}$ neutrální prvek,

prvek *b* se nazývá *prvek inverzní* (symetrický) k prvku *a*, pokud platí $aOb = bOa = e$,

e) *uzavřená* na $\boldsymbol{M}$, pokud ke každým dvěma prvkům $a, b \in \boldsymbol{M}$ je přiřazen právě jeden prvek $aOb \in \boldsymbol{M}$ [pokud provedeme binární operaci *O* mezi všemi možnými dvojicemi prvků množiny $\boldsymbol{M}$, a výsledky budou opět prvky z $\boldsymbol{M}$, je operace *O* na $\boldsymbol{M}$ uzavřená].

Pozn.: Uzavřenost operace operace plyne z definice (binární) operace.

Multiplikační (Cayleyho) tabulka

Vzájemné interakce prvků množiny v rámci dané operace můžeme přehledně znázornit pomocí takzvané *multiplikační tabulky*. Mějme například množinu $\boldsymbol{M} = \{e, a, b, c, d\}$ s operací *O*, kde prvek *e* označuje neutrální prvek vzhledem k operaci *O*. Známe-li pravidla pro počítání s prvky, můžeme sestavit multiplikační tabulku jako je tabulka Tab. 2.5 níže.

Tab. 2.5. Ukázka multiplikační tabulky (pětiprvková cyklická grupa)

O	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Záhlaví a předhlaví jsou vyplněny prvky množiny $\boldsymbol{M}$, které jsou v daném řádku (sloupci) zastoupeny právě jednou. Do levého horního políčka zpravidla píšeme označení dané operace (tedy v našem případě O).

Výsledky binární operace O se nachází v poli výsledků, které je znázorněno šedou barvou. Způsob hledání výsledků operací je totožný s hledáním výsledku součinu dvou přirozených čísel v tabulce malé násobilky, se kterým se čtenář seznámil již na prvním stupni základní školy. Tedy například prvek cOd se nachází na průniku řádku, odpovídajícímu prvku c, a sloupce, odpovídajícímu prvku d. Tedy podle tabulky Tab. 2.5 je $cOd = b$.

Pokud bychom nevěděli, že e je neutrální prvek, poznali bychom to z multiplikační tabulky. Jelikož prvky po dané operaci O s neutrálním prvkem zůstanou nezměněny, stačí najít řádek, který kopíruje záhlaví. V našem případě je to řádek druhý, který patří prvku e. Tedy e je opravdu neutrální prvek.

Víme, že výsledek operace xOx^{-1} (kde x je prvek množiny $\{e, a, b, c, d\}$) je roven prvku neutrálnímu, tedy e. Při hledání inverze budeme postupovat následovně: Najdeme neutrální prvek v příslušném řádku prvku, ke kterému chceme hledat prvek inverzní. Prvek záhlaví, který přísluší sloupci, protínající nalezený neutrální prvek výsledkového pole, je hledaný inverzní prvek.

Všimněme si, že pokud je operace O komutativní, projeví se tato skutečnost v symetrii multiplikační tabulky podle hlavní diagonály. Uzavřenost operace O se projeví ve výsledkovém poli, kde musí být v políčkách pouze prvky z množiny $\{e, a, b, c, d\}$.

Následující tabulky znázorňují některé vlastnosti operací algebraických struktur (nejedná se vždy o grupy) s nosičem $\boldsymbol{M} = \{a, b, c\}$. Na těchto příkladech je zobrazen postup hledání inverzních, neutrálních prvků a významná políčka multiplikativní tabulky.

Tab. 3.3a. Komutativnost operace O na $\boldsymbol{M}$

O	a	b	c
a	c	a	b
b	a	c	a
c	b	a	c

Tab. 3.3b. Neutrální prvek operace O na $\boldsymbol{M}$

O	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

Tab. 3.3c. Inverzní prvky operace O na $\boldsymbol{M}$

O	a	b	c
a	a	a	b
b	a	b	c
c	b	c	c

Tab. 3.3d. Neasociativnost operace O na $\boldsymbol{M}$

O	a	b	c
a	a	a	c
b	b	c	b
c	c	b	c

Komentář: Tabulka Tab. 3.3a znázorňuje komutativní operaci O. Výsledkové pole tabulky je symetrické podle hlavní diagonály (v tomto případě diagonála $O - c - c - c$ tabulky). Prvky tabulky jsou odlišeny odstíny šedi k zdůraznění sledované symetrie.

V tabulce Tab. 3.3b je zvýrazněn šedou barvou sloupec (resp. řádek), který kopíruje předhlaví (resp. záhlaví) tabulky. Odtud je zřejmé, že prvek a množiny $\boldsymbol{M}$ je neutrální vůči operaci O.

V tabulce Tab. 3.3c je vyznačen postup hledání inverze prvku a. V této tabulce je prvek b neutrální, tzn. inverze k prvku a je prvek c.

Poslední tabulka Tab. 3.3d je příkladem neasociativní operace. Protože například $aO(bOb) = c$ je různé od $(aOb)Ob = a$. V tomto případě multiplikativní tabulka operace O pomůže při ověřování asociativnosti operace O. Jelikož je však počet všech možných kompozicí prvků velký, je ověřování vlastnosti asociativnosti dané operace dosti zdlouhavé již pro operaci na třech prvcích.

Mocniny

Mějme neprázdnou množinu $\boldsymbol{M}$, prvek $a \in \boldsymbol{M}$ a přirozené číslo n. Nechť O je asociativní operace, definovaná na množině $\boldsymbol{M}$ a e je neutrální prvek množiny $\boldsymbol{M}$ vůči operaci O. Definujme *přirozenou n-tou mocninu čísla a* jako

$$a^n = \underbrace{aOaOaOaOaO \ldots Oa}_{\text{n krát}}.$$

Prvek a potom nazýváme *základ mocniny* (mocněnec). Číslo n nazýváme *exponent* (mocnitel).

Nechť je operace O na množině $\boldsymbol{M}$ s inverzními prvky. Potom můžeme dodefinovat *celočíselnou k-tou mocninu prvku a* jako prvek a^k (kde $k \in \mathbb{Z}$), pro který platí

$$a^{-k} = (a^k)^{-1}, \qquad \text{[záporné mocniny]}$$

$$a^0 = e. \qquad \text{[nultá mocnina]}$$

Vlastnosti celočíselných mocnin

Pro další užití zmiňme některé vlastnosti celočíselných mocnin. Mějme k, $l \in \mathbb{Z}$.

1. Nechť $e \in \boldsymbol{M}$ je neutrální prvek množiny $\boldsymbol{M}$ vůči asociativní operaci O, potom platí

   $$e^k = eOeOeO \ldots Oe = e,$$

   [Slovně: Mocnina neutrálního prvku je rovna neutrálnímu prvku.]

2. Nechť je operace O na množině $\boldsymbol{M}$ asociativní, potom platí

   $$a^k O a^l = (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{k krát}}) O (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{l krát}}) = (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{k + l krát}}) = a^{k+l},$$

   [Slovně pro multiplikativní zápis: Součin mocnin je roven mocnině prvku na součet exponentů.]

3. Nechť je operace O na množině $\boldsymbol{M}$ opět asociativní, potom platí

   $$(a^k)^l = (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{k krát}}) O (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{k krát}}) O \ \ldots \ O (\underbrace{aOaOaOaOaO \ldots Oa}_{\text{k krát)}} =$$

   $$= \underbrace{aOaOaOaOaO \ldots Oa}_{\text{kl krát}} = a^{kl},$$

   [Slovně pro multiplikativní zápis: Mocnina mocniny prvku je rovna mocnině na součin exponentů.]

Věta (O dělení se zbytkem): Zobrazení, které každé uspořádané dvojici celých čísel $[a, b]$ $(b \neq 0)$ přiřazuje uspořádanou dvojici $[q, r]$ celých čísel tak, že platí

$$a = bq + r, \text{ kde } 0 \leq r < |b|,$$

nazveme *dělením se zbytkem* v množině všech celých čísel $\mathbb{Z}$.

Při $r \neq 0$ číslo q nazýváme neúplný podíl čísel a, b. Číslo r nazýváme nejmenší nezáporný zbytek čísla a při dělení číslem b.

Pozn.: Speciálně pro $r = 0$ mluvíme o *dělení beze zbytku*.

Algebraické struktury

Je-li na neprázdné množině $\boldsymbol{M}$ definována rovnost „=“ prvků z $\boldsymbol{M}$ a nějaká operace O, nazveme matematický objekt $(\boldsymbol{M}, O, =)$ *algebraickou strukturou*.

Nejjednodušším příkladem algebraické struktury je tzv. *grupoid*, což je struktura $(\boldsymbol{M}, O, =)$, kde pro operaci O platí pouze pravidlo uzavřenosti (tedy jsou-li a, b z množiny $\boldsymbol{M}$, je i aOb z množiny $\boldsymbol{M}$).

Pokud je navíc operace O na množině $\boldsymbol{M}$ asociativní, strukturu $(\boldsymbol{M}, O, =)$ nazveme *pologrupa*. Pologrupu $(\boldsymbol{M}, O, =)$, ve které existuje neutrální prvek $e \in \boldsymbol{M}$, nazveme *monoid*.

Nejnáročnější algebraická struktura z hlediska vlastností operace O na $\boldsymbol{M}$, kterou získáme z monoidu přidáním vlastnosti existence inverzních prvků, se nazývá *grupa*. Právě tato struktura je ústředním tématem tohoto textu a jejími vlastnostmi se budeme hlouběji zabývat v následující kapitole.

Reference: [**BAM**], [**BIA**], [**COE**].

3. Konečné grupy

Grupa, abelovská grupa, aditivní a multiplikativní zápis grupy, řád grupy, vlastnosti grup.

V tomto textu se budeme zabývat především grupami konečnými a komutativními, ale setkáme se i s několika příklady grup nekonečných i těch, v nichž vlastnost komutativnosti neplatí.

Def. (Grupa): Nechť $\boldsymbol{M}$ je neprázdná množina a je definována rovnost „=“ prvků z $\boldsymbol{M}$. Nechť je definována binární operace $O:\boldsymbol{M}\times\boldsymbol{M}\to\boldsymbol{M}$, která je asociativní, existuje neutrální prvek $e\in\boldsymbol{M}$ struktury vzhledem k operaci O, ke každému prvku z $\boldsymbol{M}$ existuje prvek inverzní a pro libovolné $a,b\in\boldsymbol{M}$ je i $aOb\in\boldsymbol{M}$ (operace O je na $\boldsymbol{M}$ uzavřená). Potom algebraickou strukturu **G** = ($\boldsymbol{M}$, O, =) nazveme *grupa*, množinu $\boldsymbol{M}$ nazveme *nosič grupy*.

Def. (Abelovská grupa): Mějme grupu **G** = ($\boldsymbol{M}$, O, =). Pokud je operace O komutativní, nazveme **G** *abelovskou* (komutativní) *grupou*.

Def. (Řád grupy): Mějme grupu **G** = ($\boldsymbol{M}$, O, =). *Řádem grupy* myslíme počet prvků grupy $|\boldsymbol{G}|=|\boldsymbol{M}|$. Je-li $|\boldsymbol{G}|<\infty$, je grupa **G** konečná. V opačném případě je **G** nekonečná. (Jinými slovy: Řád grupy je počet všech různých prvků grupy, tedy počet prvků nosiče grupy.)

Aditivně zapsaná grupa

Pokud v grupě **G** = ($\boldsymbol{M}$, O, =) nahradíme operaci O znakem sčítání „+“, získáme tzv. a*ditivně zapsanou grupu*. Operaci „+“ na množině $\boldsymbol{M}$ nazveme *sčítání*, prvky $a,b\in\boldsymbol{M}$ nazveme *sčítance*, prvek $a+b\in\boldsymbol{M}$ nazveme *součet* prvků a, b. Neutrální prvek vzhledem ke sčítání na $\boldsymbol{M}$ nazveme *nulovým prvkem* a značíme 0. Inverzní prvek k prvku $a\in\boldsymbol{M}$ značíme $-a\in\boldsymbol{M}$ a nazýváme ho *prvkem opačným* k a.

Multiplikativně zapsaná grupa

Pokud v grupě **G** = ($\boldsymbol{M}$, O, =) nahradíme operaci O znakem násobení „·“, získáme tzv. *multiplikativně zapsanou grupu*. Operaci „·“ na množině $\boldsymbol{M}$ nazveme *násobení*, prvky $a,b\in\boldsymbol{M}$ nazveme *činitelé*, prvek $a\cdot b\in\boldsymbol{M}$ nazveme *součin* prvků a, b. Neutrální prvek vzhledem ke násobení na $\boldsymbol{M}$ nazveme *jednotkovým prvkem* a značíme 1. Inverzní prvek k prvku $a\in\boldsymbol{M}$ značíme $a^{-1}\in\boldsymbol{M}$ a nazýváme ho *prvkem převráceným* k a.

Tab. 3.1. Tabulka grup a jiných algebraických struktur

Struktura	**Jde o grupu?**
($\mathbb{N}$, +, =)	není grupa (neexistují opačné prvky ke všem prvkům z $\mathbb{N}$)
($\mathbb{N}$, ·, =)	není grupa (neexistují převrácené prvky ke všem prvkům z $\mathbb{N}$)
($\mathbb{Z}$, + =)	komutativní aditivní grupa celých čísel
($\mathbb{Z}\setminus\{0\}$, ·, =)	není grupa (neexistují převrácené prvky ke všem prvkům z $\mathbb{Z}$)
($\mathbb{Q}$, +, =)	komutativní aditivní grupa racionálních čísel
($\mathbb{Q}\setminus\{0\}$, ·, =)	komutativní multiplikativní grupa racionálních čísel
($\mathbb{Q}^+$, ·, =)	komutativní multiplikativní grupa kladných racionálních čísel
($\mathbb{Q}^-$, ·, =)	není grupa (součin dvou čísel z $\mathbb{Q}^-$ nepatří do $\mathbb{Q}^-$)
($\mathbb{R}$, +, =)	komutativní aditivní grupa reálných čísel
($\mathbb{R}\setminus\{0\}$, ·, =)	komutativní multiplikativní grupa reálných čísel
($\mathbb{C}$, +, =)	komutativní aditivní grupa komplexních čísel
($\mathbb{C}\setminus\{0\}$, ·, =)	komutativní multiplikativní grupa komplexních čísel
({0}, +, =)	komutativní aditivní grupa (0 je zároveň nulový i opačný prvek)
({1}, ·, =)	komutativní multiplikativní grupa (1 je jednotkový i převrácený prvek)
($\boldsymbol{GL}_3(\mathbb{R})$, +, =)	komutativní aditivní grupa regulárních matic typu 3×3 , kde „+“ označuje sčítání matic po prvcích (nulovým prvkem je jednotková matice typu 3×3 , opačnou maticí k matici $\boldsymbol{A}$, jejíž prvky jsou a_{jk} (kde $j, k\in\{1, 2, 3\}$), je matice -$\boldsymbol{A}$, jejíž prvky jsou -a_{jk})
($\boldsymbol{GL}_3(\mathbb{R})$, ·, =)	(nekomutativní) multiplikativní grupa regulárních matic typu 3×3
($\boldsymbol{P}(\boldsymbol{M})$, ∪ , =)	kde $\boldsymbol{P}(\boldsymbol{M})$ je množina všech podmnožin neprázdné množiny $\boldsymbol{M}$ (tzv. *potenční množina*), ∪ je binární operace sjednocení množin a „=“ je rovnost množin, **není** komutativní grupa. Neutrálním prvkem je sice prázdná množina $\emptyset\in\boldsymbol{P}(\boldsymbol{M})$. Inverzní prvky však k daným podmnožinám neexistují.

Věta (Vlastnosti grup): Mějme grupu **G** = ($\boldsymbol{M}$, ·, =). Pak platí následující vlastnosti:

1) Je-li $e\in\boldsymbol{M}$ jednotkový prvek, pak je určen jednoznačně,

2) je-li $a\in\boldsymbol{M}$, platí $(a^{-1})^{-1} = a$ [slovně: inverzní prvek k inverznímu prvku je daný prvek],

3) je-li $a^{-1} \in \boldsymbol{M}$ inverzní prvek k prvku $a \in \boldsymbol{M}$, je určen jednoznačně,

4) jsou-li $a, b \in \boldsymbol{M}$, pak $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ [inverzní prvek ke kompozici dvou prvků a, b je kompozice inverzních prvků b^{-1}, a^{-1}];

!!! POZOR: Pořadí inverzních prvků je opačné. !!!

5) jsou-li $a, b \in \boldsymbol{M}$, mají rovnice $a \cdot x = b$, $x \cdot a = b$ jednoznačná (obecně různá) řešení v $\boldsymbol{M}$,

6) jsou-li $a, x, y \in \boldsymbol{M}$, platí

$$(a \cdot x = a \cdot y) \Rightarrow (x = y) \quad \text{[tzv. věta o krácení zleva]},$$

$$(x \cdot a = y \cdot a) \Rightarrow (x = y) \quad \text{[tzv. věta o krácení zprava]}.$$

◄ Důkaz věty o vlastnostech grup

ad 1) (Důkaz sporem) Kdyby existovaly v grupě $\mathbf{G} = (\boldsymbol{M}, \cdot, =)$ dva různé inverzní prvky $e, e' \in \boldsymbol{M}$ ($e \neq e'$), pak by musely platit následující dvě rovnosti, které vyplývají z vlastnosti neutrálního prvku grupy.

$$e \cdot e' = e,$$

$$e \cdot e' = e'.$$

Dáme-li tyto dvě rovnice dohromady, získáme rovnost $e = e'$, což je spor s předpokladem $e \neq e'$. Tedy inverzní prvek grupy je určen jednoznačně.

ad 2) Je-li $a^{-1} \in \boldsymbol{M}$ inverzní prvek k prvku $a \in \boldsymbol{M}$, pak platí $a \cdot a^{-1} = a^{-1} \cdot a = e$. Což znamená zároveň, že prvek $a \in \boldsymbol{M}$ je inverzí prvku $a^{-1} \in \boldsymbol{M}$, tedy $(a^{-1})^{-1} = a$.

ad 3) Budeme dokazovat větu: $\forall a, b \in \boldsymbol{M}, (a \cdot b = e) \Rightarrow (b = a^{-1})$. Předpokládejme, že $a \cdot b = e$. Potom z vlastností neutrálního prvku $e \in \boldsymbol{M}$ a za použití asociativního zákona, který v grupách platí, je $a = a \cdot e = a \cdot (b \cdot b^{-1}) = (a \cdot b) \cdot b^{-1}$. Nyní stačí jen využít předpokladu a dosadit ho. Tedy $(a \cdot b) \cdot b^{-1} = e \cdot b^{-1} = b^{-1}$, což znamená, že jediný prvek a, splňující rovnost $a \cdot b = e$ je pouze prvek inverzní k prvku b. Nyní by bylo třeba dokázat ještě platnost věty $\forall a, b \in \boldsymbol{M}, (b \cdot a = e) \Rightarrow (b = a^{-1})$. Její důkaz je však analogický k tomuto.

Ad 4) Platí-li rovnost $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ (kde $a, b \in \boldsymbol{M}$), pak prvek $a \cdot b$ je inverzní k prvku $b^{-1} \cdot a^{-1}$ a platí $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e$ (kde $e \in \boldsymbol{M}$ označuje jednotkový prvek). Využitím asociativního zákona získáme

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot (b^{-1} \cdot a^{-1})) = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e.$$

Dospěli jsme tedy k závěru, že prvek $a \cdot b \in \boldsymbol{M}$ je inverzní k prvku $b^{-1} \cdot a^{-1} \in \boldsymbol{M}$. Tedy

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

Ad 5) Nejprve dokážeme větu $\forall a, b \in \boldsymbol{M} \; \exists x \in \boldsymbol{M}, a \cdot x = b$. Musíme dokázat, že řešení rovnice existuje a zároveň, že je toto řešení jednoznačné. Mějme prvky $a, b \in \boldsymbol{M}$; z vlastností neutrálního prvku $e \in \boldsymbol{M}$ a asociativnosti operace „·“ plyne

$$b = e \cdot b = (a \cdot a^{-1}) \cdot b = a \cdot (a^{-1} \cdot b),$$

označme $x = a^{-1} \cdot b$ řešení rovnice $a \cdot x = b$. Z vlastností grup, a zejména použitím vlastnosti 3), plyne, že prvek $a^{-1} \cdot b \in \boldsymbol{M}$ existuje a je určen jednoznačně. Věta $\forall a, b \in \boldsymbol{M} \; \exists x \in \boldsymbol{M}, a \cdot x = b$ se dokáže analogicky.

ad 6) Předpokládejme, že $\forall a, x, y \in \boldsymbol{M}, a \cdot x = a \cdot y$. Opět použijeme vlastnosti asociativnosti a neutrálního prvku $e \in \boldsymbol{M}$

$$x = e \cdot x = (a^{-1} \cdot a) \cdot x = a^{-1} \cdot (a \cdot x).$$

Nyní je čas využít předpokladu $a \cdot x = a \cdot y$, takže

$$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y) = (a^{-1} \cdot a) \cdot y = e \cdot y = y.$$

Došli jsme tedy k závěru, že $x = y$, pokud $a \cdot x = a \cdot y$ (tzv. zákon krácení zleva). Druhá věta (tzv. zákon krácení zprava) $\forall a, x, y \in \boldsymbol{M}, x \cdot a = y \cdot a$ se dokáže analogicky. ►

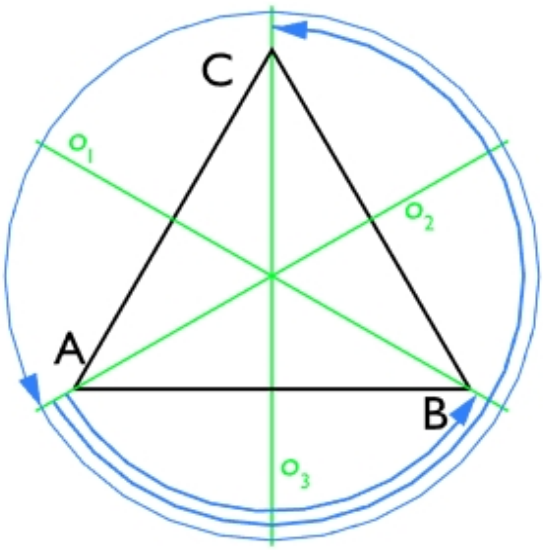
Pozn.: V každém řádku (resp. sloupci) výsledkového pole multiplikační tabulky se musí nacházet neutrální prvek právě jednou (kdyby chyběl, neexistoval by k danému prvku prvek inverzní; kdyby jich bylo naopak více, nebyl by inverzní prvek k danému prvku určen jednoznačně).

Příklad 3.1.:

Mějme libovolný rovnostranný trojúhelník ABC. Vezměme množinu všech symetrií tohoto rovnostranného trojúhelníka $\boldsymbol{M} = \{I, r_{120}, r_{240}, o_1, o_2, o_3\}$, kde I značí identitu (nebo rotaci kolem těžiště o 360°), r_{120} a r_{240} značí rotace trojúhelníka o 120 a 240 stupňů kolem těžiště proti směru hodinových ručiček. Přidejme ještě osové symetrie podle os o_1, o_2, o_3, což jsou ve skutečnosti přímky, procházející výškami trojúhelníka ABC. Všechny symetrie trojúhelníku ABC jsou znázorněny v obrázku Obr. 3.1 níže.

Zvolme nyní operaci O skládání symetrií množiny $\boldsymbol{M}$, která je v podstatě skládání zobrazení. Po provedení pár pokusů zjistíme, že výsledky operace O jsou opět prvky množiny $\boldsymbol{M}$. Můžeme se tedy pokusit vyplnit celou multiplikační tabulku operace O.

Obr. 3.1. Symetrie rovnostranného trojúhelníka ABC s těžištěm T



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Tedy například složením rotací r_{120} a r_{240} vznikne rotace trojúhelníka o 360 stupňů, což je identita I. Složením osové symetrie o_1 a identity I je opět osová symetrie o_1. Takto doplníme všechna zbývající pole multiplikační tabulky, která je pro kontrolu znázorněna tabulkou Tab. 3.2.

Tab. 3.2. Multiplikační tabulka operace O skládání symetrií rovnostranného trojúhelníka

O	I	r_{120}	r_{240}	o_1	o_2	o_3
I	I	r_{120}	r_{240}	o_1	o_2	o_3
r_{120}	r_{120}	r_{240}	I	o_3	o_1	o_2
r_{240}	r_{240}	I	r_{120}	o_2	o_3	o_1
o_1	o_1	o_2	o_3	I	r_{120}	r_{240}
o_2	o_2	o_3	o_1	r_{240}	I	r_{120}
o_3	o_3	o_1	o_2	r_{120}	r_{240}	I

Při studiu tabulky zjistíme, že operace O je na množině $\boldsymbol{M}$ asociativní, identita I je neutrální prvek, ke každému prvku množiny $\boldsymbol{M}$ existuje prvek inverzní a operace O není komutativní. Tedy algebraická struktura $\mathbf{G} = (\boldsymbol{M}, O, =)$ je příklad nekomutativní grupy.

Reference: [**GOA**], [**COE**], [**BAM**], [**BIA**].

4. Podgrupy a cyklické grupy

Podgrupa, cyklická grupa, generátor grupy, řád prvku grupy.

Def. (Podgrupa): Mějme grupu **G** = (***M***, *O*, =). Strukturu **H** = (***N***, *O*, =) nazveme *podgrupou* grupy **G**, pokud $N \subset M$ ($N \neq \emptyset$), a platí-li následující podmínky:

1) Jsou-li $c, d \in N$, pak i $cOd \in N$, [uzavřenost zúžené operace]

2) je-li $c \in N$, pak i $c^{-1} \in N$. [uzavřenost zúžené operace vůči inverzi]

Označení: **H** ≤ **G** [čteme: Grupa **H** je podgrupou grupy **G**].

Pozn. 1: Podgrupa grupy **G** je podstruktura, která má ty vlastnosti grupy **G**, které z ní samotné dělají grupu. Podmínka 1) nám říká, že podgrupa je uzavřená vůči operaci *O*. V podmínce 2) se podgrupě **H** přidává vlastnost existence inverzních prvků. Vlastnost asociativnosti se z grupy **G** dědí automaticky. Neutrální prvek $e \in M$ bude zároveň i neutrálním prvkem v množině **N** (plyne z podmínky 2) a uzavřenosti operace *O* na množině ***N***).

Pozn. 2: Je-li grupa **G** komutativní, jsou komutativní i všechny její podgrupy.

Věta (Triviální, nevlastní podgrupy): Každá grupa **G** = (***M***, *O*, =) s neutrálním prvkem $e \in M$ vůči operaci *O* na množině ***M*** má *triviální podgrupu* **E** = ({*e*}, *O*, =) a *nevlastní podgrupu* **G**.

◄ Důkaz

a) Je zřejmé, že sama grupa **G** splňuje podmínky 1) i 2) definice podgrupy, které jsou pouze zúžením definice grupy. Dále $M \subset M$ a $M \neq \emptyset$. Tedy grupa **G** je podgrupou sebe sama: **G** ≤ **G**.

b) Ověříme požadavky definice podgrupy na strukturu **E** = ({*e*}, *O*, =).

Tedy $\{e\} \subset M$ platí; $e \neq \emptyset$ platí, $eOe \in M$ platí. Inverzní prvek k (jedinému) prvku *e* struktury **E** je opět prvek *e*. Tedy i struktura **E** je podgrupou grupy **G** (**E** ≤ **G**). ►

Tab. 4.1. Příklady podgrup a jiných algebraických struktur

Struktura	Jde o podgrupu dané grupy?
({-2, -1,0, 1, 2}, +, =)	není podgrupa grupy ($\mathbb{Z}$, +, =), jelikož není splněna podmínka 1) definice podgrupy; zvolená podmnožina není uzavřená vůči operaci +
({0, 1}, +, =)	není podgrupa grupy ($\mathbb{Z}$, +, =), jelikož není splněna ani podmínka 1), ani podmínka 2) definice podgrupy
({-1, 0, 1}, +, =)	není podgrupa grupy ($\mathbb{N}$, +, =), jelikož číslo -1 není přirozené
$(\langle -1, 0\rangle \cup \langle 0, 1\rangle \subset \mathbb{Q}, \cdot, =)$	nekonečná podgrupa nekonečné grupy ($\mathbb{Q}\setminus\{0\}$, ·, =)
({7k, $k \in \mathbb{Z}$ }, +, =)	nekonečná podgrupa nekonečné grupy ($\mathbb{Q}$, +, =)
({2k; $k \in \mathbb{Z}$ }, +, =)	nekonečná podgrupa sudých čísel nekonečné grupy ($\mathbb{Z}$, +, =)
({2k+1; $k \in \mathbb{Z}$ }, +, =))	není podgrupa grupy ($\mathbb{Z}$, +, =), chybí neutrální prvek, navíc součet dvou lichých čísel je číslo sudé

Věta (O průniku podgrup): Průnik dvou podgrup grupy **G** je opět podgrupa grupy **G**.

Pozn.: Co myslíme průnikem podgrup? Mějme grupu **G** = (***M***, *O*, =) a dvě její podgrupy **K** = (***K***, *O*, =) a **L** = (***L***, *O*, =). *Průnikem podgrup* **K** a **L** myslíme strukturu **U** = ($\boldsymbol{K} \cap \boldsymbol{L}$, *O*, =).

◄ **Důkaz:** Mějme grupu **G** = (***M***, *O*, =) a dvě její podgrupy **K** = (***K***, *O*, =) a **L** = (***L***, *O*, =). Vytvoříme nyní strukturu **U** = ($\boldsymbol{K} \cap \boldsymbol{L}$, *O*, =) a ověříme, zda-li splňuje požadavky, kladené na podgrupu grupy **G**.

1) Když $\boldsymbol{K}, \boldsymbol{L} \in \boldsymbol{M}$, pak i jejich průnik $\boldsymbol{K} \cap \boldsymbol{L}$ bude určitě podmnožinou nosiče ***M*** grupy **G**. Tento průnik je navíc neprázdný, jelikož každá podgrupa grupy **G** obsahuje neutrální prvek $e \in \boldsymbol{M}$ vůči operaci *O*, tedy $e \in \boldsymbol{K} \cap \boldsymbol{L}$.

2) Co se týče inverzních prvků, je jasné, že pokud prvek $a \in \boldsymbol{K}$, je i prvek inverzní $a^{-1} \in \boldsymbol{K}$. A pokud $a \in \boldsymbol{L}$, je $a^{-1} \in \boldsymbol{L}$ (z vlastností podgrup). Bude-li tedy prvek *a* patřit do průniku množin $\boldsymbol{K} \cap \boldsymbol{L}$, bude tam automaticky patřit i jeho inverzní prvek a^{-1}. Podmínka 2) definice podgrupy je splněna.

3) Mějme prvky $a, b \in \boldsymbol{K}$. Z definice podgrupy je i prvek *aOb* v množině ***K***. Jsou-li $a, b \in \boldsymbol{K}$ zároveň prvky nosiče ***L*** podgrupy **L**, je prvek *aOb* zároveň prvkem nosiče **L**. Jinými slovy: Jsou-li prvky $a, b \in \boldsymbol{K} \cap \boldsymbol{L}$, je i prvek $aOb \in \boldsymbol{K} \cap \boldsymbol{L}$. Tedy i podmínka 1) definice podgrupy je splněna.. ►

Pozn. 1: Jelikož i podgrupa libovolné grupy je zároveň grupa, platí pro podgrupy stejná pravidla, která byla zmíněna u grup. Lze vytvářet i podgrupy podgrup. Přičemž i podgrupa podgrupy dané

grupy **G** je zároveň podgrupou grupy **G**.

Pozn. 2: Každá podgrupa libovolné grupy **G** = (***M***, *O*, =) obsahuje vždy triviální podgrupu **E** = ({*e*}, *O*, =), kde *e* je neutrální prvek grupy **G** vůči operaci *O*. Grupa **E** je nejmenší podgrupa, kterou lze v dané grupě vytvořit.

Pozn. 3: Věta o průniku podgrup se dá zobecnit na libovolný počet podgrup. Jinými slovy: Průnik libovolného systému podgrup dané grupy **G** je opět podgrupa grupy **G**.

Příklad 4.1.:

Pokud bychom podgrupy dané grupy **G** sjednocovali, pak obvykle neplatí, že výsledkem je podgrupa **G**. Například: Sjednotíme-li podgrupu ({7*k*; $k \in \mathbb{Z}$ }, +, =) a podgrupu sudých čísel ({2*k*; $k \in \mathbb{Z}$ }, +, =) grupy ($\mathbb{Q}$, +, =), získáme nosič ***M*** = {7*k*, 2*k*; $k \in \mathbb{Z}$ } struktury **U** = (***M***, +, =). Algebraická struktura **U** však není uzavřená vůči operaci + na množině ***M***, protože např. 2 + 7 = 9, což není násobek 2 ani 7.

Cyklická grupa a cyklická podgrupa

Nyní se budeme zabývat speciálním druhem podgrup, kterým jsou tzv. *cyklické grupy*. Pro přehlednost označme pro exponenty $j, k \in \mathbb{Z}$ pravidla pro celočíselné mocniny

$$(1.4.1) \qquad a^j O a^k = a^k O a^j = a^{j+k}$$

[kompozicí dvou mocnin prvku *a* je prvek *a* umocněný na součet dílčích mocnitelů],

$$(1.4.2) \qquad (a^j)^k = (a^k)^j = a^{j \cdot k}$$

[mocnina mocniny prvku *a* je prvek *a* umocněný na součin dílčích mocnitelů].

Def. (Řád prvku grupy): Mějme grupu **G** = (***M***, *O*, =) a prvek $a \in \boldsymbol{M}$. Nechť $e \in \boldsymbol{M}$ je neutrální prvek grupy **G** vůči operaci *O*. Nejmenší číslo $n \in \mathbb{N}$, pro které je $a^n = e$, nazveme *řád prvku a* grupy **G**. Značíme $o(a) = n$ (z anglického slova *order*), a čteme řád prvku *a* je roven číslu *n*.

Pozn.: Je-li řád prvku $a \in \boldsymbol{M}$ $o(a) = n$, všechny prvky, které získáme mocněním prvku *a* tvoří množinu $\boldsymbol{N} = \{e, a, a^2, a^3, a^4, ..., a^{n-1}\}$, v níž jsou prvky navzájem odlišné.

Každá mocnina prvku *a* je rovna nějakému prvku z množiny ***N***. Máme-li mocninu a^l (kde $l \in \mathbb{N}, l > n$), můžeme vyjádřit číslo *l* jako $l = n \cdot q + r$ (kde $n, q \in \mathbb{N}; r \in \mathbb{Z}$ a $0 \leq r < n$). Pak za použití pravidel (1.4.1) a (1.4.2)

$$(1.4.3) \qquad a^l = a^{n \cdot q + r} = (a^n)^q \cdot a^r.$$

Víme, že $a^n = e$ z definice řádu prvku, takže $a^l = e \cdot a^r = a^r$. Jelikož je $0 \leq r < n$, je prvek a^r roven jednomu z prvků množiny ***N***.

Pozn.: Z rovnosti (1.4.3) je zřejmé, že $a^l = e$, právě když $o(a) | l$.

Řešený příklad:

Zjistěte řád prvku $a \in \boldsymbol{M}$ grupy **G** = (***M*** = {*e*, *a*, *b*, *c*, *d*}, *O*, =), kde pravidla pro operaci *O* jsou znázorněna v multiplikační tabulce Tab. 2.5.

Řešení: Budeme umocňovat prvek *a*; řádem prvku bude první exponent $k \in \mathbb{N}$, kdy $a^k = e$. Z multiplikační tabulky je tedy $a^1 = a$, $a^2 = b$, $a^3 = c$, $a^4 = d$, $a^5 = e$. Odtud $o(a) = 5$.

Příklad 4.2.: Neutrální prvek *e* libovolné grupy **G** má řád 1, $o(e) = 1$.

Příklad 4.3.: Prvek $1 \in \mathbb{Z}$ má v aditivní grupě ($\mathbb{Z}$, +, =) řád roven nekonečnu, $o(1) = \infty$.

Příklad 4.4.: Prvek $1 \in \mathbb{Q} \setminus \{0\}$ má v multiplikativní grupě ($\mathbb{Q} \setminus \{0\}$, ·, =) řád roven 1, $o(1) = 1$.

Věta 1.4.1: Mějme grupu **G** = (***M***, *O*, =), prvek $a \in \boldsymbol{M}$, pak struktura **H** = ($\{a^i,\ i \in \mathbb{Z}\}$, *O*, =) je podgrupou grupy **G**.

◄ **Důkaz:** Ověříme požadavky, vztahující se na podgrupy. Nechť **G** = (***M***, *O*, =) je grupa, prvek $a \in \boldsymbol{M}$ a označme **H** = (***N*** = $\{a^i,\ i \in \mathbb{Z}\}$, *O*, =).

1) Je zřejmé, že množina ***N*** je neprázdná, když obsahuje přinejmenším neutrální prvek a^0. Jelikož ***N*** obsahuje pouze všechny mocniny prvku $a \in \boldsymbol{M}$, je podmnožinou množiny ***M***, která je obsahuje též.

2) Dále platí, že ke každému $a^i \in \boldsymbol{N}$ (kde $i \in \mathbb{Z}$) existuje $(a^i)^{-1} \in \boldsymbol{N}$, což plyne z faktu, že $(a^i)^{-1} = a^{-i} \in \boldsymbol{N}$. Tedy podmínka 2) definice podgrupy platí.

3) Nakonec: Po provedení operace *O* na libovolné dvě mocniny $a^j, a^k \in \boldsymbol{N}$ (kde $j, k \in \mathbb{Z}$) vznikne prvek $a^j O a^k = a^{j+k}$, který je pouze dalším prvkem (mocninou), obsaženým v množině ***N***. Tím platí i podmínka 1) definice podgrupy. ►

Def. (Cyklická podgrupa): Grupu **H** z věty 1.4.1 nazýváme *cyklickou podgrupou* grupy **G** = (***M***, *O*, =). Prvek $a \in \boldsymbol{M}$ nazveme *generátorem podgrupy* **H** a fakt, že prvek *a* generuje podgrupu **H**, zapisujeme **H** = $\langle a \rangle$.

Def. (Cyklická grupa): Mějme grupu **G** = (***M***, *O*, =). Existuje-li v množině ***M*** takový prvek *a*, že $\langle a \rangle$ = **G**, nazveme grupu **G** *cyklickou*, prvek *a* nazveme *generátor grupy* **G**.

Pozn. 1: Každý prvek cyklické grupy se dá vyjádřit jako celočíselná mocnina generátoru grupy s tím, že nultá mocnina označuje neutrální prvek grupy vůči definované operaci na nosiči grupy.

Pozn. 2: Zřejmě platí, že řád cyklické grupy **G** = $\langle a \rangle$ je roven řádu generátoru grupy a, z čehož plyne, že $|\mathbf{G}| = |\langle a \rangle| = o(a)$.

Pozn. 3: Mějme cyklickou grupu $\langle a \rangle$. Pak existují dva základní modely v závislosti na řádu grupy. Je-li $o(a) = n$, kde $n < \infty$, nazveme $\langle a \rangle$ konečnou cyklickou grupou. V opačném případě se $\langle a \rangle$ nazývá nekonečnou cyklickou grupou.

Příklad 4.6.: ($\mathbb{Z}$, +, =) je nekonečná cyklická grupa. Generátorem je pouze prvek 1 nebo -1.

Příklad 4.7.: **E** = ({e}, O, =), kde e značí neutrální prvek vůči operaci O, je konečná cyklická grupa, kterou generuje prvek e.

Příklad 4.8.: Grupa **E** z příkladu 4.7. je konečnou cyklickou podgrupou každé (obecné) grupy **G** = (***M***, O, =) s neutrálním prvkem $e \in \boldsymbol{M}$.

Příklad 4.9.: Struktura ({$10k$; $k \in \mathbb{Z}$}, +, =) je nekonečnou cyklickou podgrupou nekonečné cyklické grupy ($\mathbb{Z}$, +, =).

Řešený příklad: Dokažte, že komutativní grupa **P** = (***P*** = {♠, ♣, ♥, ♦, ☻}, O, =), kde symboly ♠, ♣, ♥, ♦, ☻ značí (po řadě) pik, tref, srdce, káro a smajlík, je cyklická. Pravidla pro operaci O jsou znázorněna v multiplikační tabulce Tab. 4.2.

Tab. 4.2. Multiplikační tabulka operace O grupy **P**

O	♠	♣	♥	♦	☻
♠	♣	♥	♦	☻	♠
♣	♥	♦	☻	♠	♣
♥	♦	☻	♠	♣	♥
♦	☻	♠	♣	♥	♦
☻	♠	♣	♥	♦	☻

Podle definice cyklické grupy musí v množině ***P*** existovat prvek, jehož postupným umocňováním získáme všechny prvky ***P***. Zkusíme tedy každý zvlášť

♠: $♠^0 = ☻$, $♠^1 = ♠$, $♠^2 = ♣$, $♠^3 = ♣O♠ = ♥$, $♠^4 = ♥O♠ = ♦$, $♠^5 = ♦O♠ = ☻$

♣: $♣^0 = ☻$, $♣^1 = ♣$, $♣^2 = ♦$, $♣^3 = ♦O♣ = ♠$, $♣^4 = ♠O♣ = ♥$, $♣^5 = ♥O♣ = ☻$

♥: $♥^0 = ☻$, $♥^1 = ♥$, $♥^2 = ♠$, $♥^3 = ♠O♥ = ♦$, $♥^4 = ♦O♥ = ♣$, $♥^5 = ♣O♥ = ☻$

♦: $♦^0 = ☻$, $♦^1 = ♦$, $♦^2 = ♥$, $♦^3 = ♥O♦ = ♣$, $♦^4 = ♣O♦ = ♠$, $♦^5 = ♠O♦ = ☻$

☻: $☻^0 = ☻$, $☻^1 = ☻$, $☻^2 = ☻$

Grupa **P** je cyklická. Generuje ji každý z prvků jejího nosiče; tedy **P** = ⟨♠⟩ = ⟨♣⟩ = ⟨♥⟩ = ⟨♦⟩.

Věta 1.4.2: Každá cyklická grupa je (komutativní) abelovská.

◄ **Důkaz**: Mějme cyklickou grupu $\langle a \rangle = (\{a^k,\ k \in \mathbb{Z}\},\ O,\ =)$. Zvolme libovolné prvky nosiče a^r, a^s (kde r, s jsou pevně zvolená celá čísla). Podle pravidla (1.4.1) platí, že $a^r O a^s = a^s O a^r$. Cyklická grupa $\langle a \rangle$ je komutativní. ►

Věta (O podgrupách cyklických grup): Každá podgrupa cyklické grupy je cyklická.

◄ **Důkaz**: Nechť $\langle a \rangle = (\{a^k,\ k \in \mathbb{Z}\},\ O,\ =)$ je cyklická grupa generovaná prvkem a. Zvolme netriviální podgrupu **H** = (***N***, O, =) grupy $\langle a \rangle$. Je zřejmé, že všechny prvky nosiče ***N*** jsou nějaké mocniny prvku a. Označme $t \in \mathbb{N}$ nejmenší exponent prvku a, že a^t patří do množiny ***N***. Existence t je zaručena, jelikož přinejmenším a^1 patří do ***N***.

Budeme se snažit dokázat, že ***N*** = $\langle a^t \rangle$. Zvolme libovolný prvek $x \in \boldsymbol{N}$. Jelikož platí, že H ≤ $\langle a \rangle$, existuje $m \in \mathbb{Z}$, pro které je $x = a^m$. Podle věty o dělení se zbytkem existuje $q, r \in \mathbb{Z}$, že $m = q \cdot t + r$ (kde $0 \le r < t$). Tedy $a^m = a^{qt} \cdot a^r$. Použijeme-li pravidla krácení, které v grupách platí, získáme

$$a^r = a^{-qt} \cdot a^m, \text{ kde } a^r \text{ patří do nosiče } \boldsymbol{N}.$$

Z faktů $0 \le r < t$ a $t \in \mathbb{N}$ je nejmenší exponent prvku a, pro který a^t patří do množiny ***N***, vyplývá, že r se musí rovnat nule. Potom $m = q \cdot t$ a prvek $x = a^m = (a^t)^q$. Což znamená, že libovolný prvek $x \in \boldsymbol{N}$ se dá vyjádřit jako celočíselná mocnina prvku a^t, tedy grupa **H** = $\langle a^t \rangle$ je cyklická podgrupa cyklické grupy $\langle a \rangle$. ►

Reference: [**WAI**], [**GOA**], [**BIA**], [**GAI**].

5. Rozklad grupy

Ekvivalence, rozklad grupy podle podgrupy, třídy rozkladu grup, Lagrangeova věta.

V této kapitole zavedeme pojmy týkající se rozkladu grupy podle podgrupy. Postupně se tak dostaneme k dalším zajímavým vlastnostem grup a dojdeme k významnému tvrzení v podobě tzv. Lagrangeovy věty.

Def. (Ekvivalence): Je-li relace $\boldsymbol{R}$ reflexivní, symetrická a tranzitivní, nazveme ji *ekvivalence*.

Def. (Rozklad množiny): Mějme množinu $\boldsymbol{M}$ a systém jejích podmnožin $\boldsymbol{N} = \{\boldsymbol{M}_r,\ r \in \mathbb{N}_k\}$. Platí-li $\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \boldsymbol{M}_3 \cup \ldots \cup \boldsymbol{M}_k = \boldsymbol{M}$ a pro každé dvě množiny $\boldsymbol{M}_p, \boldsymbol{M}_q$ (kde $p, q \in \mathbb{N}_k$) je průnik $\boldsymbol{M}_p \cap \boldsymbol{M}_q$ roven prázdné množině nebo platí $\boldsymbol{M}_p = \boldsymbol{M}_q$, pak $\boldsymbol{N}$ nazveme *rozkladem množiny* $\boldsymbol{M}$. Množiny $\boldsymbol{M}_r \in \boldsymbol{N}$ nazýváme *třídy rozkladu* množiny $\boldsymbol{M}$.

Def. (Třída ekvivalence): Mějme množinu $\boldsymbol{M}$ a na ní ekvivalenční relaci $\boldsymbol{R}$. Množinu $\boldsymbol{M}_a = \{x \in \boldsymbol{M}, x\, \boldsymbol{R}\, a\}$ nazveme *třídou množiny* $\boldsymbol{M}$ *podle ekvivalence* $\boldsymbol{R}$ danou prvkem a.

Věta (O rozkladu množiny podle ekvivalence): Nechť $\boldsymbol{R}$ označuje ekvivalenční relaci na množině $\boldsymbol{M}$. Mějme třídy ekvivalence $\boldsymbol{M}_a$ pro všechny prvky $a \in \boldsymbol{M}$. Pak množina $\boldsymbol{N} = \{\boldsymbol{M}_a, a \in \boldsymbol{M}\}$ tvoří rozklad množiny $\boldsymbol{M}$.

Pozn.: Věta říká, že pokud rozdělíme množinu $\boldsymbol{M}$ do „částí“ tak, že v každé z nich jsou prvky navzájem ekvivalentní (v relaci $\boldsymbol{R}$), vznikne rozklad množiny $\boldsymbol{M}$ a „části“ jsou vlastně třídy rozkladu.

◄ **Důkaz:** Předpokládejme, že $\boldsymbol{R}$ je ekvivalenční relace na $\boldsymbol{M}$, $\boldsymbol{M}_a = \{x \in \boldsymbol{M}, x\, \boldsymbol{R}\, a\}$ jsou podmnožiny množiny $\boldsymbol{M}$ pro každé $a \in \boldsymbol{M}$ a mějme množinu $\boldsymbol{N} = \{\boldsymbol{M}_a, a \in \boldsymbol{M}\}$.

Důkaz má dvě části:

1) Dokážeme, že je sjednocení množin $\boldsymbol{M}_a$ $\forall a \in \boldsymbol{M}$ rovno množině $\boldsymbol{M}$.

Relace $\boldsymbol{R}$ je reflexívní, tedy $\forall a \in \boldsymbol{M}$, $a\boldsymbol{R}a$. Jestli je prvek a v množině $\boldsymbol{M}$, musí být i v množině $\boldsymbol{M}_a$. Sjednocením všech množin $\boldsymbol{M}_a$ (pro všechny $a \in \boldsymbol{M}$) pak získáme množinu $\boldsymbol{M}$.

2) Dokážeme, že průnik libovolných dvou množin $\boldsymbol{M}_a$, $\boldsymbol{M}_b$ (kde $a, b \in \boldsymbol{M}$) je buď prázdná množina, nebo $\boldsymbol{M}_a = \boldsymbol{M}_b$. Předpokládejme, že průnik je neprázdný, tedy existuje třída ekvivalence $\boldsymbol{M}_x$ množiny $\boldsymbol{M}$, že $\boldsymbol{M}_a \cap \boldsymbol{M}_b = \boldsymbol{M}_x$.

Pro $\boldsymbol{M}_x$ potom z vlastností průniku množin platí $\boldsymbol{M}_x = \{x \in \boldsymbol{M}\ ,\ x\ \boldsymbol{R}\ a \wedge x\ \boldsymbol{R}\ b\}$. Z vlastnosti symetrie a tranzitivity relace $\boldsymbol{R}$ tedy můžeme usoudit, že i $a\boldsymbol{R}b$, tedy $\boldsymbol{M}_x = \boldsymbol{M}_a = \boldsymbol{M}_b$. ►

Značení: Rozklad množiny $\boldsymbol{M}$ na třídy podle ekvivalence $\boldsymbol{R}$ značíme $\boldsymbol{M}/\boldsymbol{R}$.

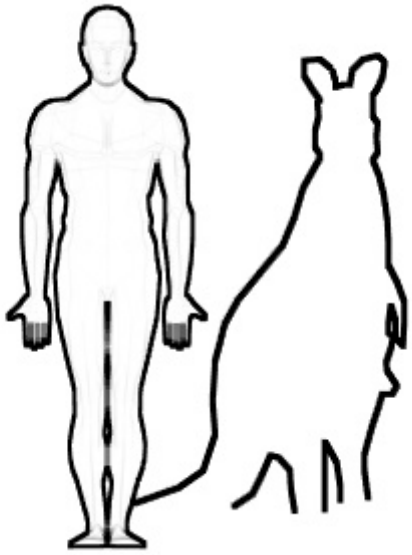
Příklad 5.1.: Mějme množinu $\boldsymbol{M}$ = {množina všech suchozemských savců na Zemi}[1]. Definujme binární relaci $\boldsymbol{N} := \forall a, b \in \boldsymbol{M}, (a\ \boldsymbol{N}\ b) \Leftrightarrow$ (savec a má stejný počet nohou jako savec b). Je zřejmé, že relace $\boldsymbol{N}$ je ekvivalence, jelikož je reflexívní, symetrická i tranzitivní. Podle věty o rozkladu množiny podle ekvivalence můžeme tedy množinu $\boldsymbol{M}$ rozložit na třídy ekvivalence $\boldsymbol{N}$. Jak budou tyto třídy vypadat?

$\boldsymbol{M}2$ = {sem budou spadat všichni savci chodící po dvou}

$\boldsymbol{M}4$ = {množina všech čtyřnožců}

Množinu $\boldsymbol{M}$, která čítá několik miliard prvků, jsme rozdělili na dvě podmnožiny, kde jsou si prvky (savci) „rovni“ ve smyslu ekvivalence $\boldsymbol{N}$.

Obr. 5.1. Třída ekvivalence $\boldsymbol{M}2$ z příkladu 5.1.



(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Přestože toho lidé a klokani nemají mnoho společného, v našem příkladě jsou bráni jako sobě rovni z hlediska relace $\boldsymbol{N}$ – lidé i klokani jsou bipedální savci, takže podle relace $\boldsymbol{N}$ je jakýkoliv klokan ekvivalentní s jakýmkoliv člověkem. Podobně je to i ve třídě $\boldsymbol{M}4$ čtyřnohých savců.

1 Do množiny $\boldsymbol{M}$ v tomto příkladě nepočítám savce, kteří se narodili bez končetin nebo o nějakou během svého života přišli (v těchto případech by bylo tříd rozkladu více).

Příklad 5.2.: Mějme grupu ($\mathbb{Z}$, +, =) a definujme na množině (nosiči) $\mathbb{Z}$ binární relaci $\equiv_3$ tak, že $\forall a, b \in \mathbb{Z}, (a \equiv_3 b) \Leftrightarrow 3|(b+(-a))$. Ověříme, zda-li je tato relace ekvivalencí.

1. Je zřejmé, že $\equiv_3$ je reflexívní, jelikož $3|0$.

2. Pokud je relace $\equiv_3$ symetrická, musí platit $\forall a, b \in \mathbb{Z}, (a \equiv_3 b) \Rightarrow (b \equiv_3 a)$, tedy $\forall a, b \in \mathbb{Z}, 3|(b+(-a)) \Rightarrow 3|(a+(-b))$. Podle věty o dělení, jestliže $3|(b+(-a))$, pak $\exists k \in \mathbb{Z}, b+(-a)=3 \cdot k$. Musíme tedy najít $l \in \mathbb{Z}$, že $a+(-b)=3 \cdot l$. Použijme tedy obě rovnice a pokusme se vyjádřit *l*. Z rovnice $b+(-a)=3 \cdot k$ vyjádříme *a*: $b=3 \cdot k+a$. To samé uděláme i v rovnici $a+(-b)=3 \cdot l$: $(-b)=3 \cdot l+(-a)$. Potom $b=-(3 \cdot l+(-a))=-3 \cdot l+a$. Dáme-li obě rovnice dohromady, získáme $3 \cdot k+a=-3 \cdot l+a$. Odtud l = -k. Číslo $l \in \mathbb{Z}$ existuje, tedy $3|(a+(-b))$, resp. $b \equiv_3 a$.

3. Ukážeme, že $\equiv_3$ je tranzitivní, tedy $\forall a, b, c \in \mathbb{Z}, (a \equiv_3 b) \wedge (b \equiv_3 c) \Rightarrow (a \equiv_3 c)$. Nechť $(a \equiv_3 b), (b \equiv_3 c)$, potom $\exists k, l \in \mathbb{Z}, (b+(-a))=3 \cdot k, (c+(-b))=3 \cdot l$. Vyjádříme z obou rovnic prvek *b*:

$$b=3 \cdot k+a,$$

$$b=-3 \cdot l+c.$$

Odtud potom $3 \cdot k+a=-3 \cdot l+c$. Po několika dalších menších úpravách získáme $c+(-a)=3 \cdot (k+l)$, což je pouze jiné vyjádření skutečnosti, že $a \equiv_3 c$.

Relace $\equiv_3$ je tedy ekvivalence, tudíž podle ní můžeme rozložit celou množinu $\mathbb{Z}$ na třídy ekvivalence. Navzájem ekvivalentní jsou ty prvky, které po dělení číslem 3 dávají stejný zbytek; tyto prvky potom tvoří jednu třídu ekvivalence. Třídy ekvivalence (resp. třídy rozkladu) jsou tedy 3:

[0] = {…, -12, -9, -6, -3, 0, 3, 6, 9, 12 ...},

[1] = {…, -11, -8, -5, -2, 1, 4, 7, 10, ...},

[2] = {…, -10, -7, -4, -1, 2, 5, 8, 11, ...}.

Pozn. 1: Rozklad $\mathbb{Z}/\equiv_3$ se označuje $\mathbb{Z}_3$, třídy ekvivalence se nazývají *zbytkové třídy modulo* 3. Relace $\equiv_3$ se nazývá *rovnost modulo* 3. Skutečnost, že $a \equiv_3 b$ (pro nějaké $a, b \in \mathbb{Z}$) čteme: „*a* je rovno *b* modulo 3“. Jiný zápis: $a = b$ (mod 3).

Pozn. 2: Relace $\equiv_3$ se dá zobecnit pro libovolné přirozené číslo *n* na relaci $\equiv_n$. Přičemž se dá dokázat, že $\equiv_n$ je ekvivalence. Důkaz je naprosto analogický k důkazu ekvivalenční relace $\equiv_3$ v příkladu výše a budeme se mu více věnovat v kapitole 6.

Příklad 5.3.: Mějme množinu V všech nenulových vektorů v prostoru $\mathbb{R}^3$. Definujme relaci rovnoběžnost vektorů $\parallel : \forall a, b \in V, a \parallel b \Leftrightarrow \exists k \in \mathbb{R} \setminus \{0\}, a = k \cdot b$. Relace $\parallel$ je ekvivalence (důkaz přenechám čtenáři), takže lze podle ní množinu V rozložit na třídy ekvivalence. Třídy ekvivalence tvoří všechny navzájem rovnoběžné vektory a nazývají se směry.

Podobným způsobem jako jsme rozložili množinu na třídy rozkladu podle dané ekvivalence, můžeme rozložit i nosič grupy podle podgrupy. Nejprve zavedeme významný termín třída grupy podle podgrupy.

Def. (Třídy grupy podle podgrupy): Mějme grupu **G** = (***M***, *O*, =) a její podgrupu **H** = (***N***, *O*, =), nechť $a \in \boldsymbol{M}$.

Levou třídou grupy **G** podle podgrupy **H** určenou prvkem *a* nazýváme množinu $a\mathbf{H} = \{aOh,\ h \in \boldsymbol{N}\}$.

Pravou třídou grupy **G** podle podgrupy **H** určenou prvkem *a* nazýváme množinu $\mathbf{H}a = \{hOa,\ h \in \boldsymbol{N}\}$.

Příklad 5.4.: Vezměme například grupu $\mathbb{Z}$ = ($\mathbb{Z}$, +, =), prvek $3 \in \mathbb{Z}$. Již jsme si ukázali v předešlém textu, že struktura **H** = ({$2k$; $k \in \mathbb{Z}$ }, +, =) je cyklickou podgrupou grupy $\mathbb{Z}$. Levou třídou grupy $\mathbb{Z}$ podle podgrupy **H** určenou prvkem 3 je množina $3\mathbf{H} = \{3+2k;\ k \in \mathbb{Z}\}$, která je v důsledku komutativnosti sčítání v $\mathbb{Z}$ rovna množině $\mathbf{H}3 = \{2k + 3;\ k \in \mathbb{Z}\}$, pokaždé jde o množinu všech lichých celých čísel.

Příklad 5.5.: Mějme libovolnou grupu **G** = (***M***, *O*, =) a její podgrupu **E** = ({*e*}, *O*, =), kde *e* značí neutrální prvek grupy **G** vůči operaci *O*. Levou třídou grupy **G** podle podgrupy **E** určenou prvkem *a* (kde $a \in \boldsymbol{M}$) je množina $a\mathbf{E} = \{aOe;\ a \in \boldsymbol{M}\} = \{a\}$.

Pozn. 1: Pro úspornost zápisu budeme dále v textu symbolem $n\mathbb{Z}$ označovat množinu {$n \cdot k$; $k \in \mathbb{Z}$ } pro dané přirozené číslo *n*. Tedy např. $100\mathbb{Z}$ = {…, -300, -200, -100, 0, 100, 200, 300, …}. Nosič podgrupy **H** z příkladu 5.4. výše je podle tohoto značení množina $3\mathbb{Z}$.

Pozn. 2: Množina $n\mathbb{Z}$ (pro libovolné $n \in \mathbb{N}$) neznamená levou třídu grupy $\mathbb{Z}$ podle podgrupy $\mathbb{Z}$ určenou prvkem *n*. Navíc $\mathbb{Z}$ není grupa vzhledem k operaci násobení. Symbol $n\mathbb{Z}$ tu pouze označuje množinu všech celočíselných násobků čísla *n*.

Věta (Rozklad grupy): Mějme grupu **G** = (***M***, *O*, =) a její podgrupu **H** = (***N***, *O*, =). Systém všech levých (pravých) tříd grupy **G** podle podgrupy **H** tvoří *rozklad* nosiče ***M*** na třídy.

◄ **Důkaz:** Je zřejmé, že levé i pravé třídy grupy **G** podle podgrupy **H** jsou podmnožinami nosiče ***M*** grupy **G**. Dokážeme, že sjednocením všech levých tříd grupy **G** podle podgrupy **H** získáme množinu ***M***, a že všechny tyto třídy jsou po dvou disjunktní (a pokud ne, jsou si rovny).

1. Zvolme třídu $a\mathbf{H} = \{aOh,\ h \in \boldsymbol{N}\}$ grupy **G** podle podgrupy **H** určenou prvkem $a \in \boldsymbol{M}$ z věty o rozkladu grupy. Jelikož **H** je podgrupa **G**, platí pro neutrální prvek *e* grupy **G**: $e \in \boldsymbol{N}$. Tedy třída $a\mathbf{H}$ musí obsahovat prvek *a*. Odtud $\forall x \in \boldsymbol{M}$ je sjednocení všech tříd $x\mathbf{H}$ rovno množině **M**. (Sjednocením všech tříd grupy **G** podle podgrupy **H** nemůže vyjít množina s prvky, které nejsou obsaženy v **M**, jelikož je podle definice podgrupy operace *O* v **H** uzavřená.)

2. Mějme grupy **G** = (***M***, *O*, =), **H** = (***N***, *O*, =), **H** ≤ **G**. Zvolme libovolné dvě levé třídy $a\mathbf{H} = \{aOh_1,\ h_1 \in \boldsymbol{N}\}$ a $b\mathbf{H} = \{bOh_2,\ h_2 \in \boldsymbol{N}\}$ grupy **G** podle podgrupy **H** určené prvky $a, b \in \boldsymbol{M}$.

   a) Pokud je $a = b$, jsou si třídy $a\mathbf{H}$, $b\mathbf{H}$ rovny.

   b) Nechť je tedy $a \neq b$. Vytvořme průnik tříd $a\mathbf{H} \cap b\mathbf{H} = \{y; y = aOh \wedge y = bOh,\ h \in \boldsymbol{N}\}$. Pro prvky průniku tedy platí $aOh = bOh$, což můžeme podle věty o krácení zprava přepsat na tvar $a = b$. Došli jsme ke sporu, tedy průnik je prázdný.

Důkaz věty pro pravé třídy je analogický k tomuto. Závěrem je tedy tvrzení, že systém všech levých (pravých) tříd grupy **G** podle podgrupy **H** tvoří rozklad nosiče grupy **G** na třídy. ►

Pozn.: Podobně jako jsme definovali rozklad množiny podle ekvivalence, můžeme nyní zavést pojem rozklad grupy podle podgrupy. Třídy ekvivalence jsou v tomto případě levé (pravé) třídy rozkladu dané grupy podle její podgrupy. Ne vždy platí, že rozklady dané grupy na pravé a levé třídy jsou stejné. V tomto textu budu rozklad grupy **G** podle její podgrupy **H** značit **G**/**H** s tím, že vždy uvedu, zda se jedná o rozklad na levé, či na pravé třídy.

Řešený příklad:

Mějme grupu $\mathbb{Q} = (\mathbb{Q}, +, =)$ a její podgrupu $\mathbb{Z} = (\mathbb{Z}, +, =)$. Levé třídy grupy $\mathbb{Q}$ podle podgrupy $\mathbb{Z}$ jsou množiny typu $\{a + b,\ b \in \mathbb{Z}\}$ pro každé číslo *a* z $\mathbb{Q}$. Podle věty o rozkladu grupy víme, že všechny levé třídy grupy $\mathbb{Q}$ podle podgrupy $\mathbb{Z}$ tvoří rozklad množiny $\mathbb{Q}$ na třídy ekvivalence. Jak tyto třídy vypadají?

Pro celočíselná *a* je třída rozkladu rovna množině celých čísel $\mathbb{Z}$.

Pro všechna ostatní $a = \frac{p}{q}$ (kde $p, k \in \mathbb{Z}$, $q \in \mathbb{N}$, $p \neq k \cdot q$). Třídy rozkladu těchto a jsou množiny racionálních čísel. Jsou to například:

$$[\frac{1}{2}] = \{\frac{1}{2} + b = \frac{1+2b}{2}, \text{ kde } b \in \mathbb{Z}\}$$

$$[\frac{7}{3}] = \{\frac{7}{3} + b = \frac{7+3b}{3}, \text{ kde } b \in \mathbb{Z}\}$$

$$[\frac{101}{78}] = \{\frac{101}{78} + b = \frac{101+78b}{78}, \text{ kde } b \in \mathbb{Z}\}.$$

Obecně můžeme třídy rozkladu grupy $\mathbb{Q}$ podle podgrupy $\mathbb{Z}$ vypsat

$$[\frac{p}{q}] = \{\frac{p}{q} + b = \frac{p+q \cdot b}{q}, \text{ kde } p, b \in \mathbb{Z}, q \in \mathbb{N}\}.$$

Pokud si výsledné třídy představíme jako číselné osy a vyjádříme je ve tvaru $a + \mathbb{Z}$: Pro celočíselná a jsou tyto třídy pouze posunutá celočíselná osa o celé číslo a, tedy výsledkem je opět nekonečná množina (číselná osa) celých čísel. Pro ostatní čísla a je celočíselná osa posunuta o racionální necelé číslo, což už se s celočíselnou osou neshoduje.

Příklad 5.6.: Vezměme grupu $\mathbb{Z} = (\mathbb{Z}, +, =)$ a její podgrupu $3\mathbb{Z} = (\{3k, k \in \mathbb{Z}\}, +, =)$. Levé třídy rozkladu $\mathbb{Z}/3\mathbb{Z}$ pro $a \in \mathbb{Z}$ mají tvar $a(3\mathbb{Z}) = \{a + 3k, k \in \mathbb{Z}\}$. Pokud si jich několik vypíšeme, zjistíme, že jsou pouze 3 různé:

[0] = {…, -12, -9, -6, -3, 0, 3, 6, 9, 12, …},

[1] = {…, -11, -8, -5, -2, 1, 4, 7, 10, 13, …},

[2] = {…, 10, -7, -4, -1, 2, 5, 8, 11, 14, …},

[3] = {…, -12, -9, -6, -3, 0, 3, 6, 9, 12, …} = [0],

[4] = [1], [5] = [2], [6] = [3] = [0], atd.

Příklad 5.7.: Mějme množinu všech dnů v týdnu. Přiřaďme jim hodnoty (po řadě) 1, 2, 3, 4, 5, 6, 0 a vytvořme množinu ***D*** = {1, 2, 3, 4, 5, 6, 0} těchto hodnot. Definujme operaci sčítání dnů na množině ***D***, která využívá těchto přiřazených hodnot. Tedy například při součtu pondělí a úterý sčítáme čísla 1 a 2. Výsledkem je číslo 3, které je přiřazeno středě. Při součtu pátku a soboty sčítáme čísla 5 a 6; výsledek je číslo 11, toto číslo musíme upravit pomocí modulární aritmetiky, jelikož nás zajímá pouze kolikátý je to den v týdnu. Jedná se tedy o čtvrtý den, což je čtvrtek. Na množině ***D*** tedy počítáme pomocí operace sčítání modulo 7 (viz strana 45). Označme tuto operaci $+_7$.

Tab. 5.1. Tabulka operace sčítání dnů v týdnu „$+_7$“ z příkladu 5.7.

+	**1**	**2**	**3**	**4**	**5**	**6**	**0**
1	2	3	4	5	6	0	1
2	3	4	5	6	0	1	2
3	4	5	6	0	1	2	3
4	5	6	0	1	2	3	4
5	6	0	1	2	3	4	5
6	0	1	2	3	4	5	6
0	1	2	3	4	5	6	0

Z tabulky Tab. 5.1 je vidět, že struktura **T** = (***D***, $+_7$, $=_7$), kde $=_7$ značí rovnost modulo 7, je komutativní grupa s neutrálním prvkem $0 \in \boldsymbol{D}$, který je přiřazen neděli. Při bližším pozorování zjistíme, že prvky 1, 2, 3, 4, 5, 6 generují grupu **T**, tedy **T** = $\langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$. Pokud zkusíme vytvořit levý rozklad **T**/$\langle 2 \rangle$, získáme třídy $x\langle 2 \rangle = \{x + 2^k,\ k \in \mathbb{Z}\}$ pro každé x z ***D***. Každá z těchto množin (tříd) však obsahuje všechny prvky množiny ***D***. Třída rozkladu je tedy pouze množina ***D***.

Nyní se podíváme hlouběji na vlastnosti tříd rozkladu a na jejich důsledky pro vlastnosti grup a podgrup.

Věta (Vlastnosti tříd rozkladu grupy podle podgrupy): Mějme grupu **G** = (***M***, *O*, =), prvky $a, b \in \boldsymbol{M}$ a grupu **H** = (***N***, *O* =), **H** ≤ **G**. Nechť jsou *a***H**, *b***H**, **H***a*, **H***b* libovolné levé a pravé třídy rozkladu **G**/**H**. Potom platí

a) $a \in b\,\mathbf{H}$, právě když $b^{-1} O a \in \boldsymbol{N}$,

b) $a \in \mathbf{H}\,b$, právě když $a\,O\,b^{-1} \in \boldsymbol{N}$,

c) *a***H** = *b***H**, právě když $b^{-1} O a \in \boldsymbol{N}$,

d) **H***a* = **H***b*, právě když $a\,O\,b^{-1} \in \boldsymbol{N}$,

e) počet prvků množiny *a***H** je roven řádu grupy **H**,

f) počet všech levých tříd rozkladu **G**/**H** je roven počtu všech pravých tříd rozkladu **G**/**H**.

◄ **Důkaz:**

ad a) Je-li $a \in b\,\mathbf{H}$, pak existuje $h \in \boldsymbol{N}$, že $a = bOh$. Násobením prvkem $b^{-1} \in \boldsymbol{M}$ zleva získáme $h = b^{-1}Oa$, což znamená, že $b^{-1} O a \in \boldsymbol{N}$.

Pokud označíme prvek $h = b^{-1} O a \in \boldsymbol{N}$, můžeme násobit tuto rovnost zleva prvkem $b \in \boldsymbol{M}$.

Získáme rovnost $a = bOh$, která podle předpokladu věty znamená, že $a \in b\mathbf{H}$. Platí tedy i obrácená implikace.

ad b) Je-li $a \in \mathbf{H}b$, pak existuje $h \in \boldsymbol{N}$, že $a = hOb$. Násobením prvkem $b^{-1} \in \boldsymbol{M}$ zprava získáme $h = aOb^{-1}$, což znamená $aOb^{-1} \in \boldsymbol{N}$.

Pokud označíme prvek $h = aOb^{-1} \in \boldsymbol{N}$, můžeme násobit obě strany této rovnosti zprava prvkem $b \in \boldsymbol{M}$. Získáme rovnost $a = hOb$, která podle předpokladu věty znamená, že $a \in \mathbf{H}b$. Platí tedy i obrácená implikace.

ad c) Předpokládejme, že $b^{-1}Oa \in \boldsymbol{N}$ platí věta a). Potom je prvek $a \in \boldsymbol{M}$ zároveň v třídě $a\mathbf{H}$ i $b\mathbf{H}$. Podle definice ale musí být třídy disjunktní, tedy $a\mathbf{H} = b\mathbf{H}$.

ad d) Zcela analogický k důkazu ad c) výše.

ad e) Dvě množiny mají stejný počet prvků, pokud existuje bijektivní zobrazení jedné na druhou. Pokud toto zobrazení najdeme, bude věta platit. Řádem podgrupy **H** myslíme počet prvků $|\boldsymbol{N}|$ množiny ***N***. Dokážeme, že zobrazení $f : \mathbf{H} \Rightarrow a\mathbf{H}$, které prvku $h \in \boldsymbol{N}$ přiřadí prvek $f(h) = aOh$ množiny $a\mathbf{H}$, je bijektivní. Pokud je $h_1 \neq h_2$ (kde $h_1, h_2 \in \boldsymbol{N}$), jsou i aOh_1, aOh_2 různé prvky třídy $a\mathbf{H}$. Zobrazení *f* je tímto prosté.

Jelikož se množina $a\mathbf{H}$ skládá pouze ze součinů aOh, je jejích prvků nejvýše $|\boldsymbol{N}|$. Protože je zobrazení *f* prosté, existuje ke každému $h \in \boldsymbol{N}$ prvek $f(h)$ z $a\mathbf{H}$. Tedy *f* je bijektivní zobrazení a platí $|\mathbf{H}| = |a\mathbf{H}| = |\boldsymbol{N}|$.

ad f) Opět budeme porovnávat velikosti dvou množin, takže hledáme bijektivní zobrazení *f* množiny ***L*** levých tříd rozkladu na množinu ***P*** pravých tříd rozkladu. Nechť $f : a\mathbf{H} \in \boldsymbol{L} \Rightarrow \mathbf{H}a^{-1} \in \boldsymbol{P}$. Pokud $u\mathbf{H}, v\mathbf{H} \in \boldsymbol{L}$ a $u\mathbf{H} \neq v\mathbf{H}$, pak pro všechna dvě čísla h_1, h_2 množiny ***N*** platí: $uOh_1 \neq vOh_2$. Odtud tedy $(uOh_1)^{-1} \neq (vOh_2)^{-1}$ a po úpravě získáme $(h_1)^{-1}O(\mathrm{u})^{-1} \neq (h_2)^{-1}O(\mathrm{v})^{-1}$. Poslední vztah však ukazuje fakt, že třídy $\mathbf{H}u^{-1}, \mathbf{H}v^{-1} \in \boldsymbol{P}$ jsou různé, tedy zobrazení *f* je prosté.

Jelikož struktura **G** je grupa, existuje ke každému prvku $a \in \boldsymbol{M}$ nosiče právě jeden prvek inverzní $a^{-1} \in \boldsymbol{M}$. Odtud je zřejmé, že množiny $\mathbf{H}a^{-1}$ pokryjí celý systém ***P***. Závěrem tedy můžeme říci, že zobrazení *f* je bijekce a počet levých i pravých tříd rozkladu **G**/**H** je stejný. ►

Pozn.: Tvrzení a), b) říkají, kdy daný prvek grupy patří do zvolené třídy rozkladu. Tvrzení c), d) ukazují způsob, jak porovnat třídy rozkladu mezi sebou. Věty e), f) popisují počet tříd a jejich prvků.

Def. (Index podgrupy v grupě): Mějme grupu **G** a nějakou její podgrupu **H**. Počet všech levých tříd grupy **G** podle podgrupy **H** nazýváme *indexem podgrupy* **H** *v grupě* **G** a značíme [**G** : **H**].

Pozn. 1: Indexem podgrupy **H** v grupě **G** myslíme počet všech levých tříd rozkladu **G**/**H**. Můžeme tedy psát $[\mathbf{G} : \mathbf{H}] = |\mathbf{G}/\mathbf{H}|$.

Pozn. 2: Z příkladu 5.5. je zřejmé, že $[\mathbf{G} : \mathbf{E}] = |\mathbf{G}|$, kde $\mathbf{E} = (\{e\}, O, =)$ je triviální podgrupa grupy **G**, *e* značí neutrální prvek grupy **G** vůči operaci *O*.

Věta (Lagrangeova): Mějme konečnou grupu **G** a nějakou její podgrupu **H**. Potom

$$|\mathbf{G}| = |\boldsymbol{H}| \cdot [\boldsymbol{G} : \mathbf{H}] .$$

◄ **Důkaz:** Z vlastností tříd rozkladu a podle věty o vlastnostech tříd rozkladu dané grupy podle její podgrupy (části e)) jsou všechny levé třídy rozkladu **G**/**H** po dvou disjunktní a mají stejný počet prvků, rovný číslu $|\mathbf{H}|$. Součtem počtů prvků všech tříd bychom měli získat počet prvků $|\mathbf{M}|$ nosiče grupy **G**, která je rovna řádu grupy **G**. Počet všech levých tříd rozkladu je roven číslu $[\mathbf{G} : \mathbf{H}] = |\mathbf{G}/\mathbf{H}|$. Odtud tedy $|\mathbf{G}| = |\boldsymbol{H}| \cdot [\boldsymbol{G} : \mathbf{H}]$.

Jelikož víme, že počet levých tříd rozkladu **G**/**H** je roven počtu pravých tříd rozkladu **G**/**H**, nemusíme větu dokazovat pro případ rozkladu **G**/**H** na pravé třídy.►

Lagrangeova věta je ve svých důsledcích velice zajímavá, a proto se na některé z nich podíváme. Připomeňme, že Lagrangeova věta platí pouze pro konečné grupy, takže se její důsledky nedají aplikovat například v nekonečné aditivní grupě celých čísel.

Důsledky Lagrangeovy věty:

Mějme konečnou grupu $\mathbf{G} = (\boldsymbol{M}, O, =)$ a její podgrupu **H**.

1) Řád podgrupy **H** dělí řád grupy **G**. Grupa **G** může tedy mít pouze podgrupy, jejichž řády jsou děliteli jejího řádu. Tento fakt ovšem neplatí obráceně: Pro každý dělitel řádu grupy **G**, nemusí nutně existovat podgrupa grupy **G**.

2) Je-li *a* prvkem grupy **G**, pak jeho řád dělí řád grupy **G**; tedy $o(a) \mid |\mathbf{G}|$. Plyne to z faktu, že řád prvku grupy je roven počtu prvků podgrupy v **G**, kterou tento prvek generuje.

3) Přímo z Lagrangeovy věty vyplývá: Je-li řád grupy **G** prvočíselný, pak jedinými jejími podgrupami je nevlastní podgrupa **G** a triviální podgrupa $\mathbf{E} = (\{e\}, O, =)$, kde *e* značí neutrální prvek grupy **G** vůči operaci *O* na ***M***.

4) Pokud je řád grupy **G** roven prvočíslu *p,* je **G** cyklická, a každý prvek různý od neutrálního generuje grupu **G**.

◄ **Důkaz:** Je-li prvek $a \in \mathbf{G}$ různý od neutrálního prvku grupy **G**, pak podgrupa $\langle a \rangle$, kterou *a* vygeneruje, musí mít podle Lagrangeovy věty řád roven prvočíslu *p*. ►

Pozn.: Z poznatků předešlé kapitoly můžeme říci i to, že kromě toho, že grupy prvočíselných řádů jsou cyklické, jsou navíc všechny i abelovské.

Věta (Základní věta cyklických grup): Nechť **G** = $\langle a \rangle$ je cyklická grupa řádu *n* (kde *n* je číslo přirozené), potom každá její podgrupa je cyklická a má řád dělící číslo *n*. Navíc ke každému přirozenému číslu *k*, které dělí řád *n* grupy **G**, existuje právě jedna podgrupa řádu *k*, která je generována mocninou $a^{n/k}$, tj. podgrupa $\langle a^{n/k} \rangle$.

Pozn.: Základní věta cyklických grup plyne z věty o podgrupách cyklických grup na straně 29 a důsledků Lagrangeovy věty.

Podoba konečných cyklických grup

Pomocí Lagrangeovy věty a základní věty cyklických grup tedy můžeme studovat podgrupy konečných cyklických grup. Mějme například cyklickou grupu $\boldsymbol{C}_{28}$ řádu 28 s generátorem *a*. Z Lagrangeovy věty plyne, že každá podgrupa této grupy musí mít řád, který dělí číslo 28. Jde o podgrupy řádu 28, 14, 7, 4, 2 a 1. Dělitelů čísla 28 je šest, to znamená, že i počet možných podgrup grupy $\boldsymbol{C}_{28}$ je šest. Možnými generátory těchto podgrup můžou být prvky (po řadě) a, a^2, a^4, a^7, a^{14}, a^{28}. Každá grupa má triviální podgrupu řádu 1, takže jedna z šesti podgrup grupy $\boldsymbol{C}_{28}$ bude triviální grupa **E** = (*e*, *O*, =), kde *O* značí operaci grupy $\boldsymbol{C}_{28}$ a *e* značí neutrální prvek grupy vůči operaci *O*. Dále víme, že každá grupa má nevlastní podgrupu. Takže podgrupa řádu 28 bude zřejmě grupa $\boldsymbol{C}_{28}$.

Dále můžeme zjistit, kolik je v grupě $\boldsymbol{C}_{28}$ prvků daného řádu pomocí takzvané Eulerovy funkce φ. Tato funkce každému přirozenému číslu *n* přiřadí číslo, které je rovno počtu všech nesoudělných přirozených čísel menších než je číslo *n*. Například φ(9) = 6, protože s devítkou je nesoudělných šest čísel {1, 2, 4, 5, 7, 8}. Pro úplnost je dodefinováno φ(1) = 1. Jelikož φ(28) = 12, existuje v grupě $\boldsymbol{C}_{28}$ 12 prvků řádu dvanáct. Podobně φ(14) = 6 znamená, že v grupě $\boldsymbol{C}_{28}$ je 6 prvků řádu 14. Z definice Eulerovy funkce plyne, že existuje pouze jeden prvek řádu 1, což je očividně prvek neutrální *e*.

Reference: [**BIA**], [**GOA**].

6. Isomorfismus grup

Isomorfismus grup, grupa zbytkových tříd $\mathbb{Z}_n$.

V této kapitole se budeme zabývat „porovnáváním“ grup pomocí mocného nástroje isomorfismu.

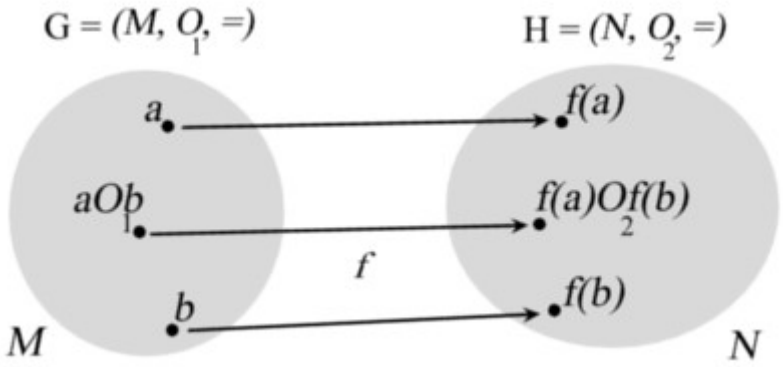
Def. (Isomorfismus grup): Mějme dvě grupy **G** = (***M***, O_1, =) a **H** = (***N***, O_2, =). Bijektivní zobrazení *f*, které zobrazí množinu ***M*** na množinu ***N***, nazveme *isomorfismem*, právě když pro všechna $a, b \in \boldsymbol{M}$ platí

$$f(aO_1b) = f(a)O_2f(b). \qquad \text{[tzv. zachování operace]}$$

Dvě grupy **G** a **H** nazveme *isomorfní*, právě když existuje nějaké isomorfní zobrazení, které zobrazí jednu na druhou (respektive jejich nosiče). Isomorfní grupy **G** a **H** označujeme $\mathbf{G} \simeq \mathbf{H}$ a čteme: Grupa **G** je isomorfní s grupou **H**, nebo grupy **G** a **H** jsou navzájem isomorfní.

Pozn.: Dále v textu budeme isomorfní zobrazení *f,* které zobrazuje nosič grupy **G** na nosič grupy **H**, značit *f*: **G** → **H**.

Obr.6.1. Grafické znázornění isomorfismu grup **G** a **H**



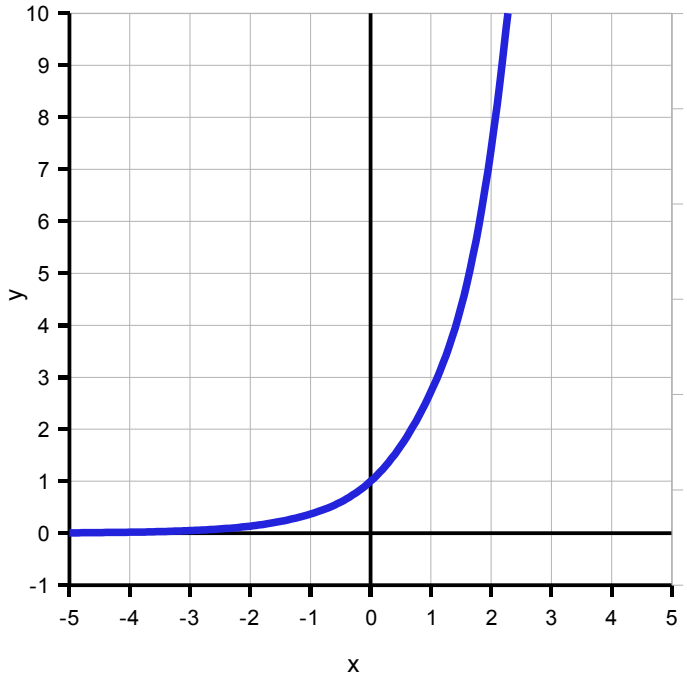
(Autor: Milan Kališ, 2007. Software: Blender 2.45)

Komentář: Obrázek nám říká, že obrazem kompozice dvou prvků *a*, *b* z množiny (nosiče) ***M*** je kompozice obrazů prvků *a*, *b* v množině (nosiči) ***N***. Důležité je nezaměňovat operace O_1, O_2 v daných nosičích ***M*** a ***N***.

Příklad 6.1.: Vezměme komutativní aditivní grupu reálných čísel a označme **R1** = ($\mathbb{R}$, +, =), komutativní multiplikativní grupu kladných reálných čísel a označme **R2** = ($\mathbb{R}^+$, ·, =), zobrazení f: $\mathbb{R} \to \mathbb{R}^+$ s předpisem $\forall a \in \mathbf{R1}; f(x) = e^x$.

Z vlastností (grafu) zobrazení $f(x) = e^x$ (viz Obr. 6.2) plyne, že zobrazení f je prosté (jedná se o exponenciálu) a ke každému bodu množiny $\mathbb{R}$ (na souřadnicové ose x =0 v grafu zobrazení f) je přiřazen bod množiny $\mathbb{R}^+$ (osa $y = 0$ v grafu zobrazení f), tedy zobrazení f je bijekce.

Obr. 6.2. Graf exponenciální funkce f: $y = e^x$



(Autor: Milan Kališ, 2008. Software: OpenOffice 2.3)

Ověřme nyní vlastností operací obou grup. Vezměme libovolné dva prvky a, b nosiče $\mathbb{R}$ grupy **R1**:

$$f(a + b) = e^{a+b}, \qquad \text{[podle předpisu zobrazení } f\text{]}$$

$$e^{a+b} = e^a \cdot e^b, \qquad \text{[podle vlastností exponenciální funkce]}$$

$$e^a \cdot e^b = f(a) \cdot f(b). \qquad \text{[podle předpisu zobrazení } f\text{]}$$

Tedy získali jsme rovnost $f(a + b) = f(a) \cdot f(b)$. Z čehož plyne, že zobrazení f je isomorfismus, tedy grupy **R1** a **R2** jsou isomorfní.

Příklad 6.2.: Zvolme grupu **G** = ({0}, +, =) a grupu **H** = ({1}, ·, =). Dále mějme zobrazení *f*, které zobrazí prvek 0 na prvek 1, *f*: {0} → {1}.

Jelikož nosiče grup **G**, **H** jsou jednoprvkové množiny, je zobrazení *f* bijekce. Zvolme libovolné dva prvky z množiny {0}. Potom platí

$$f(0 + 0) = f(0) = 1, \qquad \text{[z vlastností zobrazení } f\text{]}$$

$$1 = 1 \cdot 1 = f(0) \cdot f(0). \qquad \text{[z vlastností zobrazení } f\text{]}$$

Došli jsme k rovnosti $f(0 + 0) = f(0) \cdot f(0)$, která platí pro všechny prvky nosiče grupy **G** (jedná se pouze o prvek 0). Tedy zobrazení *f* je isomorfismus grup **G** a **H**, grupy **G** a **H** jsou isomorfní.

Příklad 6.3.: Mějme libovolnou grupu **G** = (***M***, *O*, =) a zobrazení *f*: ***M*** → ***M*** takové, že pro všechna $a \in \boldsymbol{M}$ platí,

$$f(a) = a.$$

Toto zobrazení je identita. Každý prvek se zobrazí sám na sebe, tedy zobrazení *f* je bijekce. Pro všechna *a*, *b* z množiny ***M*** navíc platí,

$$f(aOb) = aOb = f(a)Of(b).$$

Odtud vyplývá, že zobrazení *f* je isomorfismus. Jelikož jsme grupu **G** zvolili libovolně, můžeme tento poznatek zobecnit pro všechny grupy v následující poznámce.

Pozn. 1: Ke každé grupě **G** = (***M***, *O*, =) existuje zobrazení *f*: ***M*** → ***M*** s předpisem $\forall a \in \mathbf{G}$; $f(a) = a$, které je isomorfismem grupy **G** na grupu **G**. Tedy každá grupa je isomorfní sama sebou.

Pozn. 2: Isomorfismus z příkladu 6.3. se nazývá identický. Všechny isomorfismy, které zobrazují nosič grupy na sebe, se nazývají *automorfismy*.

Pozn. 3: Existence isomorfismu mezi dvěma grupami nám říká, že počet prvků nosičů obou grup je stejný. Navíc operace, definované na nosičích těchto grup, mají stejné vlastnosti. Obě grupy jsou tedy v podstatě stejné – liší se pouze „vzhledem“ prvků nosičů. Jejich multiplikační tabulky jsou přeznačené.

Pozn. 4: Relace „být isomorfní“ grup je ekvivalence, která rozkládá grupy na třídy, které potom dávají tzv. „abstraktní grupu“.

Vlastnosti isomorfismu grup

V následující větě shrneme několik základních vlastností a pravidel isomorfismu. Tyto vlastnosti jsou velkým přínosem při studiu grup. Například: Studujeme-li nějakou grupu **K**, která je isomorfní s abelovskou grupou ($\mathbb{Q}$, +, =), můžeme z jejich isomorfismu okamžitě vyvodit, že i naše studovaná grupa **K** je též abelovská, jelikož (jak se dozvíme dále v textu) isomorfismus přenáší komutativnost operací. V některých grupách je studium vlastností operací velice složité nebo časově náročné, proto je dobré nějakým způsobem dokázat, zda-li není daná grupa isomorfní s grupou, jejíž vlastnosti už dávno známe. Práce v ní je potom relativně snadnější.

Věta (Vlastnosti isomorfismu grup): Nechť jsou grupy $\mathbf{G} = (\boldsymbol{M}, O_1, =)$ a $\mathbf{H} = (\boldsymbol{N}, O_2, =)$ isomorfní, tedy existuje bijekce f: $\mathbf{G} \to \mathbf{H}$. Nechť $e_{\mathbf{G}}$ je neutrální prvek grupy **G** vzhledem k operaci O_1 a $e_{\mathbf{H}}$ je neutrální prvek grupy **H** vzhledem k operaci O_2. Pak platí:

a) Obrazem neutrálního prvku $e_{\mathbf{G}}$ grupy **G** je neutrální prvek $e_{\mathbf{H}}$ grupy **H**, tedy $f(e_{\mathbf{G}}) = e_{\mathbf{H}}$.

b) Je-li grupa **G** abelovská, je i grupa **H** abelovská. [Isomorfismus grup přenáší komutativnost operací.]

c) Nechť a je prvek grupy **G**, pak $f(a^{-1}) = f(a)^{-1}$. [Obrazem prvku inverzního k a je inverzní prvek k obrazu prvku a.]

d) Je-li **G´** podgrupa **G**, pak obraz $f(\mathbf{G}')$ je podgrupa grupy **H**. [Zachování hierarchie podgrup.]

◄ Důkaz

Předpokládejme, že grupy $\mathbf{G} = (\boldsymbol{M}, O_1, =)$ a $\mathbf{H} = (\boldsymbol{N}, O_2, =)$ jsou isomorfní.

ad a) Předpokládejme, že $e_{\mathbf{G}}$ je neutrální prvek grupy **G** vzhledem k operaci O_1 na nosiči $\boldsymbol{M}$ a $e_{\mathbf{H}}$ je neutrální prvek grupy **H** vzhledem k operaci O_2 na nosiči $\boldsymbol{N}$. Nechť a je libovolný prvek grupy **G**. Z definice isomorfismu grup plyne $f(e_{\mathbf{G}})O_2 f(a) = f(e_{\mathbf{G}} O_1 a) = f(a)$. Prvek $f(e_{\mathbf{G}})$ splňuje definici neutrálního prvku. Je tedy neutrálním prvkem na množině $\boldsymbol{N}$ vůči operaci O_2. Z vlastnosti jednoznačnosti neutrálního prvku operace tedy plyne rovnost $f(e_{\mathbf{G}}) = e_{\mathbf{H}}$.

ad b) Předpokládejme, že grupa **G** je komutativní, tedy pro všechny prvky a, b nosiče $\boldsymbol{M}$, platí $aO_1b = bO_1a$. Všechny prvky nosiče $\boldsymbol{N}$ grupy **H** jsou obrazy prvků množiny $\boldsymbol{M}$ v bijekci f, proto je tedy budeme označovat jako obrazy prvků grupy **G**. Potřebujeme tedy dokázat, že pro všechny prvky nosiče $\boldsymbol{N}$ platí $f(a)O_2 f(b) = f(b)O_2 f(a)$.

$$f(a)O_2 f(b) = f(aO_1b), \qquad [\text{isomorfismus grup } \mathbf{G} \text{ a } \mathbf{H}]$$

$$f(aO_1b) = f(bO_1a), \qquad [\text{komutativnost operace } O_1]$$

$$f(bO_1a) = f(b)O_2f(a). \qquad \text{[opět isomorfismus } \mathbf{G} \text{ a } \mathbf{H}\text{]}$$

Tedy platí $f(a)O_2f(b) = f(b)O_2f(a)$. Isomorfismus přenáší komutativnost operace.

ad c) Zde musíme dokázat, že pokud jsou grupy **G**, **H** isomorfní, pak se inverzní prvek prvku a zobrazí jako inverzní prvek prvku $f(a)$ (symbolicky $\forall a \in \boldsymbol{M}, f(a^{-1}) = f(a)^{-1}$).

Mějme neutrální prvek $e_{\mathbf{G}}$ grupy **G** vzhledem k operaci O_1 na $\boldsymbol{M}$ a neutrální prvek $e_{\mathbf{H}}$ grupy **H** vzhledem k operaci O_2 na $\boldsymbol{N}$. Nechť a je libovolný prvek grupy **G**. Potom z vlastností neutrálního prvku grupy **H** plyne:

$$f(a^{-1}) = f(a^{-1})O_2e_{\mathbf{H}} = f(a^{-1})O_2(f(a)O_2f(a)^{-1}).$$

Nyní můžeme využít asociativnosti operace O_2:

$$f(a^{-1})O_2(f(a)O_2f(a)^{-1}) = (f(a^{-1})O_2f(a))O_2f(a)^{-1}.$$

Nakonec využijeme isomorfismus grup **G** a **H** a vlastnosti neutrálního prvku grupy **G**:

$$(f(a^{-1})O_2f(a))O_2f(a)^{-1} = f(a^{-1}O_1a)O_2f(a)^{-1} = f(e_{\mathbf{G}})O_2f(a)^{-1} = e_{\mathbf{H}}O_2f(a)^{-1} = f(a)^{-1}.$$

Odtud tedy $f(a^{-1}) = f(a)^{-1}$ pro libovolný prvek grupy **G**.

ad d) Nechť $\mathbf{G}' = (\boldsymbol{M}', O_1', =)$ je podgrupa grupy $\mathbf{G} = (\boldsymbol{M}, O_1, =)$. Máme dokázat, že množina obrazů všech prvků množiny $\boldsymbol{M}'$ společně s operací O_2 tvoří podgrupu grupy **H**.

Označme $f(\boldsymbol{M}')$ množinu obrazů prvků nosiče $\boldsymbol{M}'$ grupy $\mathbf{G}'$. Množina $f(\boldsymbol{M}')$ je jistě neprázdná, jelikož z definice podgrup musí být nosič $\boldsymbol{M}'$ neprázdný a navíc isomorfismus f přiřadil každému prvku nosiče $\boldsymbol{M}$ grupy **G** (tedy i nosiče $\boldsymbol{M}'$) právě jeden prvek nosiče $\boldsymbol{N}$ grupy **H**. Odtud tedy i platí, že množina $f(\boldsymbol{M}')$ je podmnožinou nosiče $\boldsymbol{N}$ grupy **H**. Pokusme se tedy vytvořit strukturu $f(\mathbf{G}') = (f(\boldsymbol{M}'), O_2, =)$ a ověřme, zda pro ní platí podmínky 1) a 2) z definice podgrupy.

1) Operace O_1 grupy $\mathbf{G}'$ je na $\boldsymbol{M}'$ uzavřená. Ke každým dvěma prvkům $a, b \in \boldsymbol{M}'$ existují prvky $f(a), f(b) \in \boldsymbol{N}$, že (z definice isomorfismu) platí:

$$f(a)O_2f(b) = f(aO_1b).$$

Jelikož kompozice aO_1b je prvkem nosiče $\boldsymbol{M}'$, patří prvek $f(aO_1b)$ do množiny $f(\boldsymbol{M}')$. Operace O_2 je tedy na množině $f(\boldsymbol{M}')$ uzavřená.

2) Obdobně, vezmeme-li prvek $a \in \boldsymbol{M}'$, pak existuje i prvek $f(a) \in f(\boldsymbol{M}')$. Použijeme již dokázané vlastnosti c) isomorfismu grup, tedy $f(a)^{-1} = f(a^{-1})$. Jelikož ke každému prvku a nosiče M′ existuje jeho inverzní prvek v $\boldsymbol{M}'$, je prvek a^{-1} prvkem množiny $f(\boldsymbol{M}')$.

Tím jsme tedy dokázali, že struktura $f(\mathbf{G}') = (f(\boldsymbol{M}'), O_2, =)$ je podgrupou grupy **H**.►

Vlastnosti (komutativní) aditivní grupy celých čísel ($\mathbb{Z}$, +, =)

V této podkapitole se budeme věnovat některým specifickým vlastnostem grupy $\mathbb{Z} = (\mathbb{Z}, +, =)$, která je pro teorii grup velice významná. Spousta vlastností bude vlastně důsledek některých poznatků, ke kterým jsme již došli v předešlých kapitolách.

Věta: Každá podgrupa grupy $\mathbb{Z}$ je cyklická a dá se vyjádřit ve tvaru $n\mathbb{Z} = (n\mathbb{Z}, +, =)$, kde n je nezáporné číslo.

◄ Důkaz

V kapitole 4 jsme v podsekci Cyklické grupy a cyklické podgrupy již dokázali, že libovolná podgrupa cyklické grupy je cyklická, což platí i pro případ grupy $\mathbb{Z}$. Zbývá tedy dokázat, že tyto cyklické podgrupy mají tvar $n\mathbb{Z} = (n\mathbb{Z}, +, =)$.

Předpokládejme, že grupa **G** je cyklickou podgrupou grupy $\mathbb{Z}$ a prvek a je jejím generátorem (tj. $\mathbf{G} = \langle a \rangle$). Z vlastností podgrup plyne, že grupa **G** přebírá operaci „+“ grupy $\mathbb{Z}$, která je pouze „zúžena“ na nosič podgrupy **G**, tedy grupa **G** dá se zapsat jako $\mathbf{G} = (\langle a \rangle, +, =)$. Nyní si stačí jen uvědomit, že umocňováním generátoru (v našem případě celočíselným násobením) cyklické grupy získáme všechny prvky nosiče dané grupy. Pak grupu **G** můžeme zapisovat ve tvaru $\mathbf{G} = (\{a \cdot k, k \in \mathbb{Z}\}, +, =)$, což je tvar, ke kterému jsme se chtěli dostat, tedy $\mathbf{G} = (n\mathbb{Z}, +, =) = n\mathbb{Z}$.►

Grupa $\mathbb{Z}_n$ zbytkových tříd modulo *n*

V kapitole 5 jsme ukázali, že lze rozložit grupu celých čísel na třídy ekvivalence podle ekvivalenční relace $\equiv_3$ a označili jsme ji $\mathbb{Z}_3$, tedy $\mathbb{Z}_3 = \mathbb{Z} / \equiv_3$. Množina $\mathbb{Z}_3$ se skládá ze tří zbytkových tříd, vzniklých při dělení celých čísel číslem 3. Dále bylo naznačeno, že stejným způsobem se dá vytvořit množina zbytkových tříd $\mathbb{Z}_n$.

Prvky množiny $\mathbb{Z}_n$ jsou zbytkové třídy, vzniklé při dělení celých čísel přirozeným číslem n. Zbytkové třídy jsou nekonečné disjunktní množiny a mají tvar:

$[0] = [n] = \{\ldots, -n, -3n, -2n, -n, \underline{\mathbf{0}}, n, 2n, 3n, 4n, \ldots\}$

$[1] = \{\ldots, 1 - 3n, 1 - 2n, 1 - n, \underline{\mathbf{1}}, 1 + n, 1 + 2n, 1 + 3n, \ldots\}$

$[2] = \{\ldots, 2 - 3n, 2 - 2n, 2 - n, \underline{\mathbf{2}}, 2 + n, 2 + 2n, 2 + 3n, \ldots\}$

$[3] = \{\ldots, 3 - 3n, 3 - 2n, 3 - n, \underline{\mathbf{3}}, 3 + n, 3 + 2n, 3 + 3n, \ldots\}$

…

$[h] = \{\ldots, h - 3n, h - 2n, h - n, \underline{\boldsymbol{h}}, h + n, h + 2n, h + 3n, \ldots\}$

...

$[n\text{-}1] = \{\ldots, -2n - 1, -n - 1, -1, \underline{\boldsymbol{n - 1}}, 2n - 1, 3n - 1, 4n - 1, \ldots\}$,

kde h je přirozené číslo, $0 \leq h \leq n - 1$.

Jelikož pracujeme s nekonečnými množinami, bylo by dobré nějak tyto množiny označit kvůli přehlednosti a úspoře místa. Vyberme pro každou zbytkovou třídu tzv. *reprezentanta*, což bude nejmenší nezáporné celé číslo dané třídy (pro zvýraznění zobrazeno podtrženými tučnými čísly výše). Například pro třídu $\{\ldots, 2 - 3n, 2 - 2n, 2 - n, \underline{\mathbf{2}}, 2 + n, 2 + 2n, 2 + 3n, \ldots\}$ to bude číslo 2. Budeme tedy danou třídu označovat symbolem $[a]$, kde číslo a je reprezentant třídy, a číst „zbytková třída reprezentovaná číslem (prvkem) a“.

Tedy množina $\mathbb{Z}_n = \{[0], [1], [2], [3], \ldots, [h], \ldots, [n\text{-}1]\}$ je konečná a má n prvků. Vezměme nyní tuto množinu jako nosič algebraické struktury a definujme na nově vznikající struktuře operaci a rovnost prvků.

a) **Rovnost prvků**

Budeme ji značit $\equiv_n$ (slovně: rovnost modulo n). Využijeme faktu, že zbytkové třídy jsou disjunktní množiny, tedy jsou si rovny právě tehdy, když mají společný prvek. Jinými slovy: Nechť $[a]$, $[b]$ označuje libovolné třídy rozkladu v množině $\mathbb{Z}_n$, potom $\forall [a], [b] \in \mathbb{Z}_n; [a] \equiv_n [b]$, právě tehdy, když průnik $[a] \cap [b]$ je neprázdná množina.

b) **Operace na struktuře**

Nadefinujeme operaci sčítání zbytkových tříd $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$. Vezměme opět dvě libovolné zbytkové třídy $[a]$, $[b]$ nosiče $\mathbb{Z}_n$ (kde $0 \leq a; b \leq n - 1$). Potom součet dvou tříd množiny $\mathbb{Z}_n$, které jsou reprezentovány čísly a a b, je zbytková třída množiny $\mathbb{Z}_n$ reprezentovaná číslem $a + b$. Jinými slovy: $\forall [a], [b] \in \mathbb{Z}_n; [a] +_n [b] \equiv_n [a + b]$.

Pozn.: Operaci $+_n$ slovně interpretujeme jako sčítání modulo n. Přičemž je třeba dodat, že z vlastností zbytkových tříd vyplývá, že nezáleží na volbě reprezentantů, jelikož pracujeme ve skutečnosti se zbytky po dělení nějakým přirozeným číslem.

V tomto okamžiku můžeme definovat strukturu $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \equiv_n)$ a studovat její vlastnosti.

U) Uzavřenost operace $+_n$: Plyne přímo z její definice.

A) Asociativnost operace $+_n$: Jelikož sčítáme vlastně reprezentanty daných tříd, což jsou celá čísla, je asociativnost operace $+_n$ zaručena asociativností grupy $\mathbb{Z} = (\mathbb{Z}, +, =)$.

E) Neutrální prvek operace $+_n$: Snadno se ověří, že neutrální prvek operace $+_n$ je prvek (zbytková třída) $[0] = [n]$.

S) Existence opačných (symetrických) prvků: Nechť zbytková třída $[b]$ je inverzním prvkem k libovolně zvolenému prvku $[a]$. Potom $[a] + [b] = [0]$.

Pokud si opět uvědomíme, že stačí pracovat s reprezentanty zbytkových tříd, zjistíme, že je třeba spočítat pouze hodnotu celého čísla b v rovnici $a + b = 0$, což je reprezentant hledané inverzní třídy (prvku). Potom $b = -a$, tedy $[b] = [-a]$ je inverzní prvek k prvku $[a]$. Jelikož struktura $(\mathbb{Z}, +, =)$ je grupa, je existence prvků $-a$ (respektive zbytkových tříd $[-a]$) automaticky zaručena pro všechna a (respektive třídy $[a]$).

K) Komutativnost operace $+_n$: Z komutativnosti operace „+“ v grupě $\mathbb{Z}$ plyne:

$$[a] +_n [b] =_n [a + b] =_n [b + a] =_n [b] +_n [a].$$

(komentář: první rovnost vyplývá z definice operace $+_n$. Druhá rovnost je důsledkem komutativnosti operace + v grupě $\mathbb{Z}$. A třetí rovnost vyplývá opět z definice operace $+_n$ grupy $\mathbb{Z}_n$)

Tedy operace $+_n$ je i komutativní.

Shrnutí: z vlastností U) až K) plyne, že struktura $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \equiv_n)$ je abelovská grupa. Dále v textu ji budeme označovat jako grupu zbytkových tříd modulo n.

Pozn. 1: Množinu (nosič) grupy $\mathbb{Z}_n$ můžeme konstruovat rozkladem $\mathbb{Z}/n\mathbb{Z}$ způsobem, který je uveden v příkladu 5.2. pro $n = 3$. Výsledkem jsou opět určité zbytkové třídy. Dodefinování rovnosti a sčítání modulo n by probíhalo stejně jako v předešlém postupu. Nově vzniklá struktura by byla tedy opět grupa, která by byla isomorfní s grupou $\mathbb{Z}_n$.

Pozn. 2: Pro úsporu místa a času se při zápisu zbytkových tříd vynechávají hranaté závorky a místo toho se zapisují pouze reprezentanti. Například: $\mathbb{Z}_7 = (\{0, 1, 2, 3, 4, 5, 6\}, +_7, \equiv_7)$.

Věta: Každá konečná cyklická grupa řádu n je isomorfní s grupou $\mathbb{Z}_n$ (kde n je přirozené číslo).

◄ Důkaz

Mějme konečnou cyklickou grupu **G** řádu n (kde n je přirozené číslo) s generátorem x, tedy platí $\mathbf{G} = \langle x \rangle$. Označme „·“ operaci na grupě **G** a „=“ rovnost prvků na nosiči grupy **G**. Dále označme $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \equiv_n)$ jako grupu zbytkových tříd modulo n. Pokud najdeme isomorfní zobrazení grupy $\mathbb{Z}_n$ na grupu **G**, budou tyto grupy isomorfní.

1) Nechť n je libovolné přirozené číslo. Potom pro řád grupy **G** platí: $|\mathbf{G}| = |\langle x \rangle| = o(x) = n$. Tedy nosiče obou grup mají stejný počet prvků.

2) Vezměme zobrazení f: $\mathbb{Z}_n \to \mathbf{G}$, definované předpisem: $\forall a \in \mathbb{Z}_n \, \exists u \in \mathbf{G}; f(a) = u^a$, toto zobrazení je prosté, jelikož grafem zobrazení f je exponenciála (definovaná v diskrétních bodech 0, 1, 2, …, n – 1). Jedná se tedy o bijektivní zobrazení.

3) Nyní ověříme, zda jsou zachovány vlastnosti operací. Tedy nechť a, b jsou prvky grupy $\mathbb{Z}_n$. Potom

$$f(a + b) = u^{a+b}, \qquad \text{[z definice zobrazení } f\text{]}$$

$$u^{a+b} = u^a \cdot u^b, \qquad \text{[z vlastností mocnin]}$$

$$u^a \cdot u^b = f(a) \cdot f(b). \qquad \text{[z definice zobrazení } f\text{]}$$

Došli jsme k rovnosti $f(a + b) = f(a) \cdot f(b)$, tedy z odstavců 1) až 3) plyne, že zobrazení f je isomorfismus. Tedy grupy **G** a $\mathbb{Z}_n$ jsou isomorfní, věta platí.►

Pozn.: Věta nám v podstatě říká, že (až na isomorfismus) existuje pouze jediná konečná cyklická grupa řádu 1, 2, 3, …., n (pro přirozená čísla n).

Věta: Každá nekonečná cyklická grupa je isomorfní s grupou $\mathbb{Z}$.

◄ Důkaz

Mějme nekonečnou cyklickou grupu $\mathbf{G} = \langle x \rangle = (\{\ldots, x^{-2}, x^{-1}, x^0 = 1, x^1, x^2, \ldots\}, \cdot, =)$; $o(x) = \infty$. Nechť $\mathbb{Z} = (\mathbb{Z}, +, =)$ je abelovská grupa všech celých čísel.

Uvažujme zobrazení f: $\mathbb{Z} \to \mathbf{G}$, dané předpisem $f(a) = x^a$, pro celá čísla a a prvky x nosiče grupy **G**. Podívejme se nyní na některé vzory a obrazy prvků obou grup **G** a $\mathbb{Z}$: $0 \to 1$, $1 \to x^1$, $2 \to x^2$, $-1 \to x^{-1}$, $-2 \to x^{-2}$. Přestože jsou obě grupy nekonečné, každému prvku grupy $\mathbb{Z}$ můžeme vždy přiřadit pomocí předpisu f prvek nosiče grupy **G**. Jelikož je grupa **G** cyklická je každý z prvků x^k (pro celá čísla k) různý, tedy zobrazení f je zároveň i prosté. Jedná se o bijektivní zobrazení.

Pro celá čísla a, b potom z vlastností cyklických grup a definice zobrazení f platí:

$$f(a + b) = x^{a+b},$$

$$x^{a+b} = x^a \cdot x^b,$$

$$x^a \cdot x^b = f(a) \cdot f(b).$$

Rovnost $f(a + b) = f(a) \cdot f(b)$ platí. Tedy zobrazení f je isomorfismus grup **G**, $\mathbb{Z}$.►

Pozn.: Tedy (až na isomorfismus) existuje pouze jediná nekonečná cyklická grupa.

Právě díky vlastnostem popsaným v posledních dvou dokazovaných větách je grupa celých čísel velmi významnou strukturou a má smysl studovat její vlastnosti. Z Lagrangeovy věty dále vyplývá: Jelikož je grupa $\mathbb{Z}_n$ zbytkových tříd modulo n (kde n je číslo přirozené) cyklická a konečná, její podgrupy jsou konečné a cyklické a mají řád, který dělí číslo n.

Reference: [**BJ1**], [**BJ2**], [**GOA**], [**GOI**], [**KOT**], [**WAI**], [**WIK**].

7. Klasifikace grup

Permutace, grupa symetrií, diedrická grupa, Kleinova grupa, grupa kvaternionů, klasifikace grup malých řádů, direktní součin.

Další část textu bude věnovaná speciálním druhům grup. Především se budeme věnovat jejich struktuře, specifické vlastnosti těchto grup přenechám čtenáři jako objekt vlastního zkoumání a využití znalostí z předešlých kapitol tohoto textu.

I) Symetrická grupa (grupa permutací) S_n

Def. (Permutace): Nechť ***M*** je neprázdná množina. Bijektivní zobrazení σ: ***M*** $\rightarrow$ ***M*** nazveme *permutací*.

Příklad 7.1.: Mějme množinu ***M*** šesti žáků třídy ZŠ, kteří sedí na šesti židlích. V určitý okamžik se žáci musí přesadit tak, aby každý z nich seděl na právě jedné židli. Různých možností, jak si tito žáci mohou sednout je mnoho a každá z nich je permutací množiny ***M***. Jedna z těchto permutací by bylo zobrazení, které žáku A přiřadí židli žáka B, žáku B židli žáka C, žáku C židli žáka D, žáku D židli žáka E, žáku E židli žáka F a žáku F židli žáka A. Tedy, pokud množina ***M*** = {A, B, C, D, E, F} a zobrazení σ je touto permutací množiny ***M***, pak platí vztahy $\sigma(A) = B$, $\sigma(B) = C$, $\sigma(C) = D$, $\sigma(D) = E$, $\sigma(E) = F$ a $\sigma(F) = A$, nebo i jiným zápisem σ: A $\rightarrow$ B, B $\rightarrow$ C, C $\rightarrow$ D, D $\rightarrow$ E, E $\rightarrow$ F, F $\rightarrow$ A, ze kterého vyplývá, že jde o cyklus.

Příklad 7.2.: Mějme množinu ***KOŠÍK*** a v ní tři prvky: hruška, jablko, švestka. Pokud budeme ovoce po jednom z ***KOŠÍK***u vytahovat a pokládat vedle sebe zleva doprava na stůl, získáme různé trojice ovoce (prvků množiny ***KOŠÍK***). Každá z těchto trojic (kterých je dohromady šest různých) je permutací množiny ***KOŠÍK***.

Označme prvek hruška jako H, jablko jako J a švestku jako Š. Dále označme množinu ***KOŠÍK*** = {H, J, Š}.Vypišme všechny permutace množiny ***KOŠÍK***:

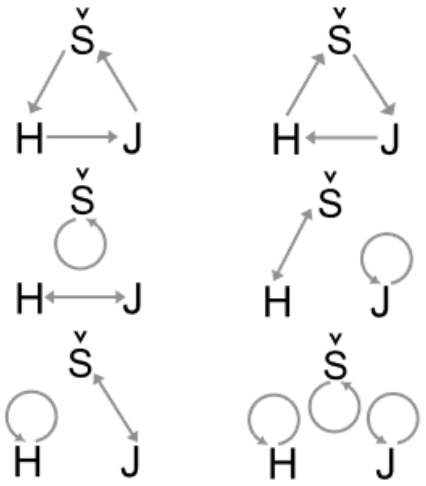
σ_1: H $\rightarrow$ J, J $\rightarrow$ Š, Š $\rightarrow$ H; σ_2: H $\rightarrow$ Š, Š $\rightarrow$ J, J $\rightarrow$ H;

σ_3: H $\rightarrow$ J, J $\rightarrow$ H, Š $\rightarrow$ Š; σ_4: H $\rightarrow$ Š, Š $\rightarrow$ H, J $\rightarrow$ J;

σ_5: H $\rightarrow$ H, J $\rightarrow$ Š, Š $\rightarrow$ J; σ_6: H $\rightarrow$ H, J $\rightarrow$ J, Š $\rightarrow$ Š.

Pro grafické znázornění se používají takzvané cykly. Pro každou permutaci se prvky dané množiny postaví do pozic vrcholů (pevných bodů) pravidelného *n*-úhelníku (kde *n* je počet prvků dané množiny). Následuje zakreslování šipek mezi prvky podle pravidel permutace. Tedy například podle permutace σ_1: H → J, J → Š, Š → H množiny KOŠÍK tvoří prvky H, J, Š rovnostranný trojúhelník a šipky jdou z H do J, z J do Š a z Š zpět do H (viz levý horní obrázek níže). Pomocí cyklů tak lze studovat jednotlivé vazby mezi prvky dané permutace lépe. Obrázek Obr. 7.1 znázorňuje cykly permutací příkladu 7.2.

Obr. 7.1. Cykly všech permutací množiny ***KOŠÍK***



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Příklad 7.3.: Mějme množinu $\mathbb{N}_k = \{1, 2, 3, \ldots, k\}$, kde *k* je číslo přirozené. Libovolné zobrazení, které zobrazí množinu $\mathbb{N}_k$ na množinu $\mathbb{N}_k^*$, kde množina $\mathbb{N}_k^*$ obsahuje každý prvek množiny $\mathbb{N}_k$ právě jednou (v libovolném pořadí), je permutací množiny $\mathbb{N}_k$.

Mějme například množinu $\mathbb{N}_7 = \{1, 2, 3, 4, 5, 6, 7\}$. A mějme permutaci σ: 1 → 1, 2 → 3, 3 → 5, 4 → 6, 5 → 7, 6 → 4, 7 → 2. Pro takovéto permutace se často používá následující dvouřádkový zápis:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 1\,3\,5\,6\,7\,4\,2 \end{pmatrix}$$

Je zřejmé, že vezmeme-li množinu šesti školáků a množinu {1, 2, 3, 4, 5, 6}, výsledné permutace

budou fakticky stejné (jelikož můžeme každému žáku přiřadit právě jedno z čísel 1 až 6 a pracovat místo s lidmi s čísly). Mějme tedy konečnou množinu $\mathbb{N}_k = \{1, 2, 3, \ldots, k\}$, kde k je číslo přirozené. Z kombinatoriky víme, že počet všech permutací množiny $\mathbb{N}_k$ je $k \cdot (k-1) \cdot (k-2) \cdot (k-3) \cdot 2 \cdot 1$. Tedy například pro desetiprvkovou množinu máme 3 628 800 různých permutací. Vytvořme množinu $\boldsymbol{M}$ všech těchto permutací a definujme na této množině operaci „skládání permutací“ a označme ji o_p. Skládání permutací probíhá stejně jako skládání běžných zobrazení. Tedy například mějme dvě permutace σ_1, σ_2 množiny $\mathbb{N}_7$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Permutace složená z těchto dvou permutací $\sigma_3 = \sigma_1 \, o_p \, \sigma_2$. Tedy platí,

σ_3: $1 \to 7 \to 1$; $2 \to 6 \to 2$; $3 \to 5 \to 3$; $4 \to 4 \to 4$; $5 \to 3 \to 5$; $6 \to 2 \to 6$; $7 \to 1 \to 7$.

Výsledná permutace σ_3 je rovna

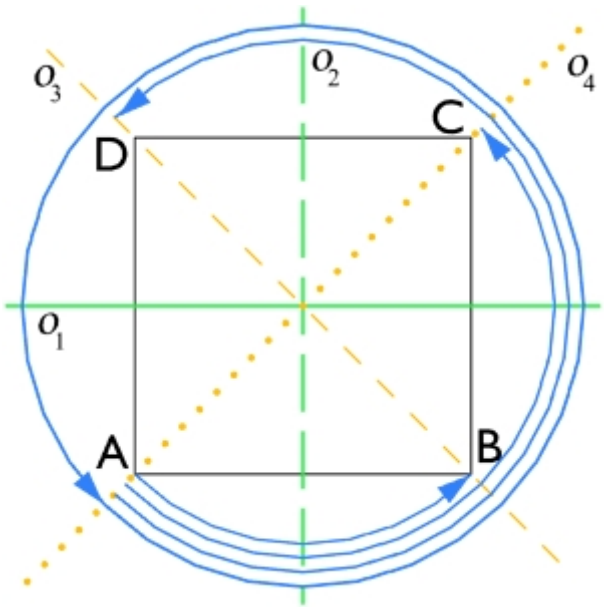
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

Množina $\boldsymbol{M}$, operace o_p a rovnost „=“ permutací na množině $\boldsymbol{M}$ vytváří grupu (důkaz přenechám čtenáři), která se pro svou významnou roli označuje jako symetrická grupa stupně n a značí se $\mathbf{S}_n$. Každou podgrupu grupy $\mathbf{S}_n$ nazýváme též grupou permutací. O symetrických grupách (grupách permutací) se ještě trochu více zmíníme v další kapitole.

II) Diedrická grupa D_n

Jedná se o grupu symetrií pravidelného n-úhelníku (pro přirozená čísla $n > 2$). Vezměme například pravidelný čtyřúhelník, čili čtverec. Čtverec má hned několik symetrií: osové (podle os o_1, o_2, o_3, o_4); rotace podle středu S ($r_1 = 90°$, $r_2 = 180°$, $r_3 = 270°$) a identickou symetrii I, která je totožná s rotací podle středu čtverce ABCD o 360 stupňů (viz obrázek Obr. 7.2)

Obr. 7.2. Grafické znázornění symetrií čtverce



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Komentář: Přímky označují osy symetrie o_1 (horizontální osa), o_2 (vertikální osa), o_3 (přímka DB), o_4 (přímka AC) čtverce ABCD. Modré čáry označují rotace $r_1 = 90°$, $r_2 = 180°$, $r_3 = 270°$ podle středu čtverce ABCD a identitu I, která je zobrazena modrou kružnicí opisující 360 stupňů.

Vytvořme nyní množinu $\boldsymbol{M}$ těchto symetrií. Všimněme si, že symetrie podle osy o_3 = DB může vzniknout složením symetrií o_2 a r_1 (v tomto pořadí), a že symetrie o_4 = AC může vzniknout složením symetrií o_1 a r_1 (v tomto pořadí). Dále můžeme vypustit symetrii r_3, která může vzniknout složením rotací r_1 a r_2. A nakonec i rotaci r_1, která může vzniknout složením symetrií o_3 (respektive o_2 složeno r_1) a o_1. Definujme množinu $\boldsymbol{M} = \{o_1, o_2, r_{180}, I\}$, kde I značí identitu.

Vytvořme strukturu $\boldsymbol{V} = (\boldsymbol{M}, \circ, =)$, kde operace $\circ$ značí skládání zobrazení (vybraných symetrií našeho čtverce). Tabulka Tab. 4 znázorňuje multiplikační tabulku této operace. Je zřejmé, že prvek I je

neutrálním prvkem množiny $\boldsymbol{M}$ vzhledem k operaci $\circ$. Dále je z tabulky Tab. 7.1 vidět, že každý prvek je inverzní k sobě samému, a že operace $\circ$ je komutativní. Asociativnost operace je zaručena asociativností operace skládání zobrazení. Operace $\circ$ je navíc na množině $\boldsymbol{M}$ uzavřená (složením dvou zobrazení množiny $\boldsymbol{M}$ vznikne opět zobrazení množiny $\boldsymbol{M}$).

Tedy struktura $\boldsymbol{V} = (\boldsymbol{M}, \circ, =)$ je komutativní grupa. Tato grupa se označuje jako *Kleinova 4-grupa* (nebo německy Vierergruppe) a je jednou z mnoha tzv. *diedrických grup*. Grupu symetrií pravidelného n-úhelníku (pro $n > 2$) budeme značit $\mathbf{D}_n$. Kleinovu grupu lze považovat za diedrickou grupu $\mathbf{D}_2$.

Tab. 7.1. Multiplikační tabulka operace „$\circ$" Kleinovy grupy $\boldsymbol{V}$

$\circ$	I	o_1	o_2	r_{180}
I	I	o_1	o_2	r_{180}
o_1	o_1	I	r_{180}	o_2
o_2	o_2	r_{180}	I	o_1
r_{180}	r_{180}	o_2	o_1	I

Diedrické grupy mají zajímavé vlastnosti a uplatnění například v biologii, nicméně jejich zkoumání již není náplní tohoto textu.

III) Grupa kvaternionů

Mějme množinu čísel $\{1, -1, i, -i, j, -j, k, -k\}$, kde platí $i^2 = j^2 = k^2 = ijk = -1$. Potom algebraická struktura $\boldsymbol{Q} = (\{1, -1, i, -i, j, -j, k, -k\}, \cdot, =)$ s operací „$\cdot$“ násobení prvků nosiče tvoří tzv. *grupu kvaternionů*. Prvek 1 je neutrálním prvkem grupy. Multiplikační tabulka operace „$\cdot$“ je zobrazena v tabulce Tab. 7.2. Pro prvky nosiče grupy $\boldsymbol{Q}$ platí následující vztahy

$$i \cdot j = k, j \cdot i = -k,$$

$$j \cdot k = i, k \cdot j = -i,$$

$$k \cdot i = j, i \cdot k = -j.$$

Tab. 7.2. Multiplikační tabulka operace „·“ grupy kvaternionů

·	1	-1	*i*	-*i*	*j*	-*j*	*k*	-*k*
1	1	-1	*i*	-*i*	*j*	-*j*	*k*	-*k*
-1	-1	1	-*i*	*i*	-*j*	*j*	-*k*	*k*
i	*i*	-*i*	-1	1	*k*	-*k*	-*j*	*j*
-*i*	-*i*	*i*	1	-1	-*k*	*k*	*j*	-*j*
j	*j*	-*j*	-*k*	*k*	-1	1	*i*	-*i*
-*j*	-*j*	*j*	*k*	-*k*	1	-1	-*i*	*i*
k	*k*	-*k*	*j*	-*j*	-*i*	*i*	-1	1
-*k*	-*k*	*k*	-*j*	*j*	*i*	-*i*	1	-1

Prvky množiny $\mathbf{H} = \{a + b\cdot i + c\cdot j + d\cdot k,\ a, b, c, d \in \mathbb{R}\}$, kde čísla *i*, *j*, *k* jsou prvky grupy $\boldsymbol{Q}$ se nazývají hamiltoniány (popř. kvaterniony) a jsou určitým zobecněním čísel komplexních. Využití nacházejí ve fyzice, matematice 4rozměrných těles a počítačové grafice.

Grupa kvaternionů je jeden z příkladů nekomutativních grup.

IV) Klasifikace grup malých řádů

Ještě než přejdeme k vlastní klasifikaci grup malých řádů (resp. řádů 1 až 8), podívejme se pro úplnost ještě na speciální druh grup, vzniklých tzv. direktním součinem grup jiných.

Def. (Direktní součin grup): Mějme dvě grupy $\mathbf{G} = (\boldsymbol{M}, o_1, =_1)$ a $\mathbf{H} = (\boldsymbol{N}, o_2, =_2)$. *Direktním součinem* grup **G** a **H** je algebraická struktura $\mathbf{G}\times\mathbf{H} = (\{(a, b), \text{ kde } a \in \boldsymbol{M}, b \in \boldsymbol{N}\}, \cdot, =)$, pro jejíž operaci součin „·“ a $\forall a, b \in \boldsymbol{M}, c, d \in \boldsymbol{N}$ platí následující formule

$$(a, c)\cdot(b, d) = (ao_1c, bo_2d).$$

Pozn.: Jedná se o algebraickou strukturu, jejíž nosič obsahuje uspořádané dvojice prvků z grupy **G** a grupy **H** (v tomto pořadí). Operace „·“ se v této struktuře řídí pravidlem popsaným v definici. Grupy **G**, **H** nemusí být nutně odlišné, můžeme vytvářet například i direktní součin $\mathbb{Z}_2\times\mathbb{Z}_2$.

Příklad 7.3.:

Mějme dvě cyklické grupy druhého řádu $\mathbf{S}_2 = (\{1, a\}, \cdot, =)$ a $\mathbf{T}_2 = (\{0, b\}, +, =)$. Vytvořme direktní součin grup $\mathbf{S}_2$, $\mathbf{T}_2$. Nosič této struktury je množina $\boldsymbol{M} = \{(1, 0), (1, b), (a, 0), (a, b)\}$. Dodefinujme na této množině operaci součin, který podléhá pravidlu v definici direktního součinu grup, a označme ji například *. Pro prvky množiny $\boldsymbol{M}$ tedy například platí $(a, 0)*(1, 0) = (a\cdot1, 0 + 0) = (a, 0)$, nebo pro jinou dvojici $(a, b)*(a, 0) = (a\cdot a, b + 0) = (1, 0)$.

Pozn. 1: Direktní součin dvou grup je opět grupa. Čtenář může ověřit sám. Prvky nosiče direktního součinu grup jsou uspořádané dvojice prvků daných grup. A jelikož operace direktního součinu pracuje s těmito prvky po složkách, přenesou se vlastnosti grup i do struktury direktního součinu.

Pro kontrolu: Mějme grupy $\mathbf{G} = (\boldsymbol{M}, o_1, =_1)$ a $\mathbf{H} = (\boldsymbol{N}, o_2, =_2)$, prvky a, 1_G patří do nosiče $\boldsymbol{M}$ a prvky b, 1_H patří do nosiče $\boldsymbol{N}$ (1_G a 1_H jsou neutrální prvky grupy **G** a **H**). Je-li (a, b) prvek direktního součinu $\mathbf{G}\times\mathbf{H}$, potom prvek k němu inverzní je $(a, b)^{-1} = (a^{-1}, b^{-1})$. Neutrálním prvkem této grupy je $(1_G, 1_H)$. Asociativnost a popřípadě i komutativnost operací je zaručena prací po složkách.

Pozn. 2: Můžeme vytvářet i vícenásobné direktní součiny grup. Tedy i například direktní součin $\mathbf{A}\times\mathbf{B}\times\mathbf{C}\times\mathbf{D}\times\mathbf{E}$ grup **A**, **B**, **C**, **D**, **E**.

Pro další část kapitoly je důležitá následující tvrzení: Nechť m, n jsou čísla přirozená větší nebo rovno dvěma. Potom grupa $\mathbb{Z}_{mn}$ je isomorfní s grupou $\mathbb{Z}_m\times\mathbb{Z}_n$, právě když jsou čísla m, n nesoudělná. Důkaz čtenář najde v publikaci [**BJ1**]. Tedy například grupa $\mathbb{Z}_{12}$ je isomorfní s grupou $\mathbb{Z}_3\times\mathbb{Z}_4$. Řád grupy $\mathbb{Z}_m\times\mathbb{Z}_n$ je tedy roven číslu $m \cdot n$.

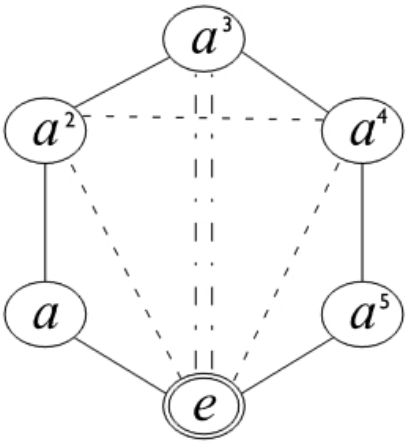
Cyklový graf grupy

Jedná se o grafické znázornění vzájemných vztahů prvků cyklické grupy. Na rozdíl od multiplikační tabulky je cyklový graf zaměřen spíše na vnitřní strukturu grupy, mocniny prvků a podgrupy, které generují. S jeho podobou jsme se již setkali u znázornění permutací.

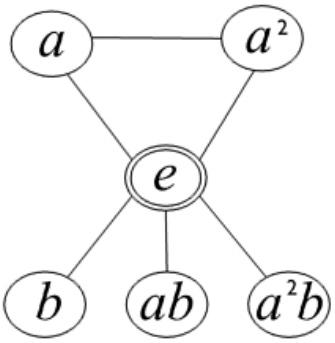
Mějme například cyklickou grupu $\mathbf{C}_6$ řádu šest s generátorem a. Mocniny prvku a vytvoří cyklus, který zakreslíme jako pravidelný šestiúhelník s mocninami prvku a ve vrcholech. Dále víme, že mocniny prvku a^2 vytvoří také cyklus, jedná se o podgrupu této grupy. Dále máme ještě jeden cyklus generovaný prvkem a^3. Poslední „speciální“ cyklus je tvořen neutrálním prvkem $e = a^0$. Tyto menší cykly znázorníme odlišným šrafováním spojnic odpovídajících mocnin. Výsledný cyklický graf je znázorněn v obrázku Obr. 7.3a.

Pokud má grupa generátorů více, znázorní se i přídavné cykly ostatních generátorů a jejich kompozic tak, že se všechny cykly spojují ve vrcholu neutrálního prvku. Příklad takového cyklového grafu je struktura generátorů diedrické grupy $\mathbf{D}_3$, což je grupa řádu 6. Cyklový graf této grupy je znázorněn na obrázku Obr. 7.3b. Jak vidíte z obrázku, je hned zřejmé, že struktury těchto dvou grup jsou zcela odlišné. Právě pro tento účel jsou cyklové grafy výhodné.

Obr. 7.3a. Cyklový graf grupy $\mathbf{C}_6$



Obr. 7.3b. Cyklový graf grupy $\mathbf{D}_3$



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Nyní jsme již připraveni na klasifikaci grup. Při studiu vlastností isomorfismu grup dojdou někteří z nás k otázce, kolik grup daného řádu vlastně existuje (až na isomorfismus) a jaké mají vlastnosti? V tomto okamžiku bych čtenáře rád odkázal na podrobnou anglickou softwarovou aplikaci *Group Explorer* (odkaz: http://groupexplorer.sourceforge.net/), která dokáže v mnoha směrech odpovědět kolikrát lépe než člověk. Produkt je sice v angličtině, ale multiplikační tabulky, grafy a zápis podgrup apod. je zpracován tak, že je ho schopen vstřebat i angličtinář-začátečník. Tato aplikace vizualizuje dokonce i cyklový graf pro danou grupu. V tomto textu bude vypsáno jen několik základních vlastností studovaných grup řádu 1 až 8, a proto odkazuji čtenáře na výše zmíněnou aplikaci a literaturu, zmíněnou na konci diplomové práce.

Jak už bylo řečeno v předešlé kapitole, každá konečná cyklická grupa řádu n je isomorfní s grupou $\mathbb{Z}_n$ (kde n je přirozené číslo). Tedy naše klasifikace bude určitě obsahovat cyklické grupy $\mathbb{Z}_1$ až $\mathbb{Z}_8$. Dále víme, že existují i další grupy – direktní součiny, takže ke grupám řádu 8 bude patřit nejen grupa $\mathbb{Z}_8$, ale například i grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$, která s grupou $\mathbb{Z}_8$ není isomorfní. Navíc jsou zde i další typy grup jako jsou diedrické grupy, které nejsou vždy isomorfní s výše zmíněnou grupou. Klasifikací grup z hlediska isomorfismu se matematici zabývali ve velké míře, takže byli schopni jejich vzájemný isomorfismus důkladně ověřit.

1) Grupy řádu 1

Do této skupiny spadá až na isomorfismus pouze grupa $\mathbb{Z}_1$. Všechny grupy 1. řádu jsou isomorfní s touto grupou. Tedy i například triviální grupa **E** = ({*e*}, *O*, =)) a jakákoliv jiná cyklická grupa řádu 1. Grupa $\mathbb{Z}_1$ je abelovská.

Pozn.: Jelikož je ve skupině grup prvního řádu pouze jeden typ grup, což je grupa cyklická, jsou i všechny grupy prvního řádu cyklické. Toto tvrzení se dá zobecnit pro všechny ostatní grupy prvočíselných řádů. Vlastnost plyne z cykličnosti grup $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, … .

2) Grupy řádu 2

Každá grupa 2. řádu je isomorfní s grupou $\mathbb{Z}_2$. Týká se to všech cyklických grup řádu 2, které jsou s ní isomorfní. Grupa $\mathbb{Z}_2$ je abelovská.

3) Grupy řádu 3

Každá grupa 3. řádu je isomorfní s cyklickou grupou $\mathbb{Z}_3$. Grupa $\mathbb{Z}_3$ je abelovská, tedy i ostatní grupy 3. řádu jsou abelovské.

4) Grupy řádu 4

V této skupině jsou dva druhy grup, které jsou navzájem neisomorfní.

a) Cyklická abelovská grupa $\mathbb{Z}_4$.

b) Řád čtyři má i Kleinova grupa *V*, která se dá pokládat za diedrickou grupu D2. Tato grupa je isomorfní s direktním součinem $\mathbb{Z}_2 \times \mathbb{Z}_2$. Multiplikační tabulka a stručný popis vlastností této grupy je na straně 52-53. Důsledkem je, že s každou grupou isomorfní s Kleinovou grupou *V*, můžeme nakládat jako s grupou symetrií čtverce. I Kleinova grupa je abelovská

5) Grupy řádu 5

Do této skupiny patří pouze grupa $\mathbb{Z}_5$. Jelikož je číslo pět prvočíslo, nebude zde jiná skupina zastoupená nějakým direktním součinem. Grupa $\mathbb{Z}_5$ je abelovská. S grupou $\mathbb{Z}_5$ jsou isomorfní například grupy ({-2, -1, 0, 1, 2}, +, =) a **P** = (***P*** = {♠, ♣, ♥, ♦, ☻}, *O*, =) z předešlých kapitol, přičemž multiplikační tabulka grupy **P** se dá použít pro libovolnou grupu 5. řádu.

6) Grupy řádu 6

Zde opět dochází ke členění.

a) V první skupině grup řádu 6 patří grupa $\mathbb{Z}_6$, což je grupa abelovská. S touto grupou je isomorfní například i direktní součin $\mathbb{Z}_3 \times \mathbb{Z}_2$.

b) Druhou skupinu tvoří diedrická grupa $\mathbf{D}_3$, která s grupou $\mathbb{Z}_6$ není isomorfní. S grupou $\mathbf{D}_3$ je isomorfní i například grupa $\mathbf{S}_3$, tedy grupa všech permutací na třech prvcích (počet permutací tří prvků je šest). Multiplikační tabulka operace této grupy je znázorněna v tabulce Tab. 3.2. Zajímavostí této skupiny je, že všechny tyto grupy nejsou komutativní (abelovské).

7) Grupy řádu 7

Grupa sedmého řádu je (až na isomorfismus) jen cyklická grupa $\mathbb{Z}_7$. Grupa $\mathbb{Z}_7$ a všechny ostatní grupy tohoto řádu jsou abelovské. S touto grupou je isomorfní například i grupa dní v týdnu v příkladě 5.7., jejíž multiplikační tabulka se dá použít pro všechny grupy této skupiny.

8) Grupy řádu 8

V této kategorii je už skupin pět.

a) Abelovská grupa $\mathbb{Z}_8$.

b) Abelovská grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$.

c) Abelovská grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, což je příklad direktního součinu více než dvou grup.

d) Do další skupiny patří (až na isomorfismus) diedrická grupa $\mathbf{D}_4$ symetrií pravidelného osmiúhelníku. Tato grupa není abelovská.

e) Poslední skupinu tvoří všechny grupy isomorfní s grupou kvaternionů $\boldsymbol{Q}$. Ani tato grupa není abelovská.

Touto cestou je možné klasifikovat grupy vyšších řádů, přičemž se zvyšujícím se řádem grupy často roste i počet neisomorfních skupin grup daného řádu. V aplikaci Group Explorer je (duben 2008) klasifikace grup až do řádu 146. Pro hlubší studium vlastností a znázornění grup malých řádů čtenáře odkazuji na tuto aplikaci.

Tab. 7.3. Klasifikace grup malých řádů

Řád grupy	Komutativní grupa	Nekomutativní grupa
1	$\mathbb{Z}_1 \simeq \mathbf{S}_1$	-
2	$\mathbb{Z}_2 \simeq \mathbf{S}_2$	-
3	$\mathbb{Z}_3$	-
4	$\mathbb{Z}_4$, $\boldsymbol{V} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$	-
5	$\mathbb{Z}_5$	-
6	$\mathbb{Z}_6$	$\mathbf{D}_3 \simeq \mathbf{S}_3$
7	$\mathbb{Z}_7$	-
8	$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbf{D}_4$, $\boldsymbol{Q}$

Reference: [**BJ1**], [**BJ2**], [**GOA**], [**GOI**], [**KOT**], [**VIV**], [**WAI**], [**WEC**], [**WIK**].

8. Reprezentace grup

Reprezentace grup, Cayleyho věta.

V této kapitole ukážeme, že stejně jako jsme rozkládali množiny na třídy podle nějaké ekvivalence, můžeme vytvořit i množinu všech možných grup a rozložit ji podle relace „být isomorfní“, která se ukáže být ekvivalencí. Již jsme si ukázali v kapitole o isomorfismu grup, že navzájem isomorfní grupy se „chovají“ stejně, takže nemá smysl studovat každou zvlášť. A to je okamžik, kdy na řadu přichází reprezentace grup. V této kapitole pouze zmíním reprezentace grupami permutací.

Jak už bylo řečeno v úvodu, pokud vytvoříme množinu, která sestává ze všech možných grup, které je lidský mozek schopen vyprodukovat, lze tyto grupy třídit pomocí relace isomorfismu.

Nyní se pokusíme dokázat, že isomorfismus grup „$\simeq$“ je ekvivalentní relace. Tedy je to relace, která je reflexívní, symetrická a tranzitivní.

Mějme množinu $\boldsymbol{\Omega}$, jejíž prvky budou všechny grupy. Tato množina je jistě neprázdná, několik příkladů jsme si již v tomto textu ukázali. Jelikož při zjišťování existence isomorfismu mezi dvěma grupami vytváříme vlastně uspořádané dvojice, je isomorfismus grup „ $\simeq$ “ relace podle definice na straně 9.

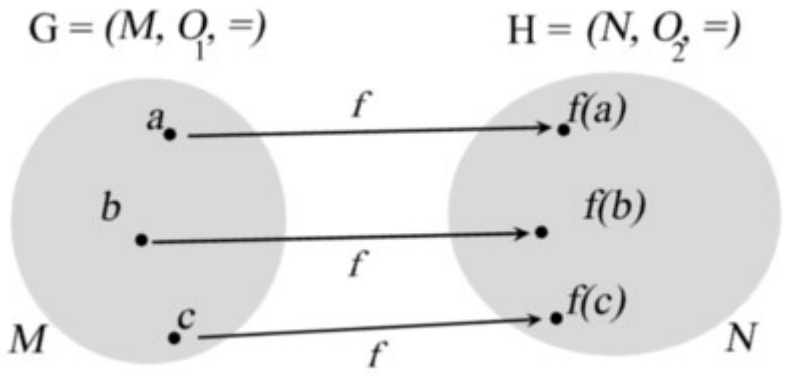
Reflexívnost: Měli bychom dokázat, že každá grupa $\mathbf{G}$ množiny $\boldsymbol{\Omega}$ všech grup je isomorfní sama se sebou (symbolicky $\forall \mathbf{G} \in \boldsymbol{\Omega}; \mathbf{G} \simeq \mathbf{G}$). Použijme tedy definice isomorfismu ze začátku minulé kapitoly. Zvolme zobrazení f: $\mathbf{G} \rightarrow \mathbf{G}$, které každému prvku $a \in \mathbf{G}$ přiřadí prvek a, tedy $f(a) = a$. Toto zobrazení je jistě prosté a každý prvek má svůj vzor i obraz. Pro operaci O_1 a prvky a, b grupy $\mathbf{G}$ platí:

$$f(a) O_1 f(b) = a O_1 b = f(a O_1 b).$$

Zobrazení f zachovává operaci, je isomorfismem. Tedy každá grupa je isomorfní sama se sebou. Isomorfismus je potom reflexívní relace.

Symetričnost: Zde bychom měli dokázat, že pokud je grupa $\mathbf{G}$ isomorfní s grupou $\mathbf{H}$, je i grupa $\mathbf{H}$ isomorfní s grupou $\mathbf{G}$ (symbolicky $\forall \mathbf{G}, \mathbf{H} \in \boldsymbol{\Omega}; \mathbf{G} \simeq \mathbf{H} \rightarrow \mathbf{H} \simeq \mathbf{G}$). Předpokládejme, že grupa $\mathbf{G}$ je isomorfní s grupou $\mathbf{H}$, tedy existuje bijektivní zobrazení f: $\mathbf{G} \rightarrow \mathbf{H}$, které zachovává operace. Odtud musíme dokázat, že existuje zobrazení g, které prvkům nosiče grupy $\mathbf{H}$ přiřadí prvky nosiče grupy $\mathbf{G}$. Využijme grafického znázornění bijekce f (viz obrázek Obr.8.1).

Obr.8.1. Znázornění isomorfního zobrazení *f*



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Zobrazení *f* je bijekce, tedy ke každé dvojici bodů z grupy **G** a grupy **H** vždy existuje právě jedna „šipka“, která je spojuje. Zobrazení *f* je prosté, tedy k němu existuje zobrazení inverzní f^{-1}, které je podle vlastností inverzních zobrazení (interpretace obrázku Obr. 8.1) také prosté. Grupy **G** i **H** mají stejný počet prvků, tedy i f^{-1} bude bijekce. Vypadá to tedy, že pokud zvolíme $g = f^{-1}$, mohli bychom se dobrat ke zdárnému cíli. Ověřme, zda bijekce f^{-1} zachovává operace. Tedy ověřme, zda platí pro všechny prvky *c*, *d* nosiče grupy **H**, že $f^{-1}(cO_2d) = f^{-1}(c)O_1 f^{-1}(d)$?

Víme, že zobrazení *f*, přiřadí každému prvku nosiče grupy **G** prvek nosiče grupy **H**. Přiřaďme tedy prvkům *c*, *d* jejich obrazy *a*, *b* v nosiči grupy **G**, tak, že $c = f(a)$ a $d = f(b)$.

Potom $f^{-1}(c)O_1 f^{-1}(d) = f^{-1}(f(a))O_1 f^{-1}(f(b))$. Nyní využijeme vlastnosti inverzních zobrazení: Vzor obrazu prvku *x* je vzor, tedy prvek *x* (symbolicky $f^{-1}(f(x)) = x$). Pak můžeme psát

$$f^{-1}(f(a))O_1 f^{-1}(f(b)) = aO_1b.$$

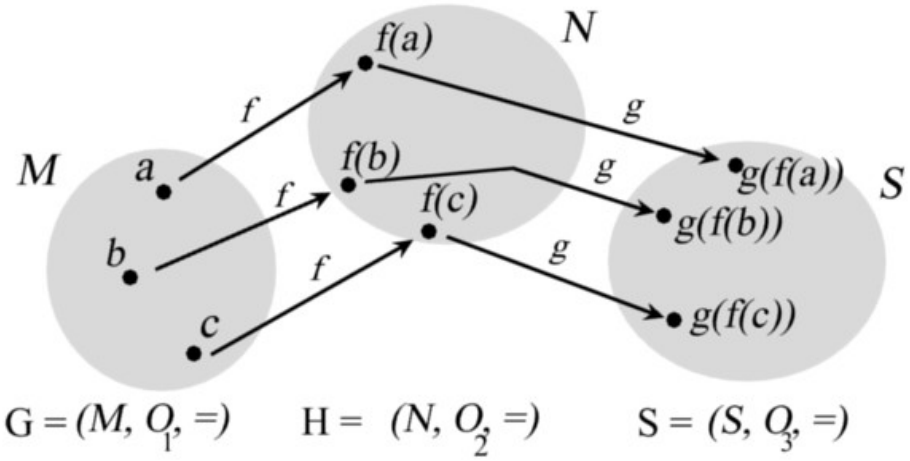
Použijme předpoklad, že zobrazení *f* zachovává operace, a vlastnost „vzor obrazu“ z minulého odstavce. Tedy $aO_1b = f^{-1}(f(aO_1b)) = f^{-1}(f(a)O_2f(b))$. Nyní si stačí uvědomit, že $c = f(a)$ a $d = f(b)$, potom můžeme psát $f^{-1}(f(a)O_2f(b)) = f^{-1}(cO_2d)$.

Pokud projdeme text zpátky, zjistíme, že jsme právě dokázali rovnost $f^{-1}(cO_2d) = f^{-1}(c)O_1 f^{-1}(d)$. Tedy zobrazení f^{-1} je nejen bijektivní, ale dokonce zachovává operace. f^{-1}: **H** → **G** je isomorfismus. Došli jsme tedy k závěru, že isomorfismus je i relace symetrická.

Tranzitivnost: Pokud aplikujeme definici tranzitivní relace na náš případ, dostaneme větu, kterou budeme dále dokazovat. Tedy pro libovolné grupy **G**, **H**, **S** množiny $\boldsymbol{\Omega}$ všech grup má platit, že, pokud je grupa **G** isomorfní s grupou **H** a grupa **H** je isomorfní s grupou **S**, je i grupa **H** isomorfní s grupou **S** (symbolicky $\forall \mathbf{G}, \mathbf{H}, \mathbf{S} \in \boldsymbol{\Omega}, (\mathbf{G} \simeq \mathbf{H} \wedge \mathbf{H} \simeq \mathbf{S}) \rightarrow \mathbf{G} \simeq \mathbf{S}$).

Předpokládejme, že $\mathbf{G} \simeq \mathbf{H}$ a $\mathbf{H} \simeq \mathbf{S}$ a označme f: $\mathbf{G} \rightarrow \mathbf{H}$ a g: $\mathbf{H} \rightarrow \mathbf{S}$. Dokážeme, že grupa **H** je isomorfní s grupou **S**, tedy musí existovat nějaké bijektivní zobrazení (označme ho h), které zachovává operace. Opět použijeme grafické znázornění (viz obrázek Obr.8.2).

Obr.8.2. Znázornění tranzitivnosti relace isomorfismus grup



(Autor: Milan Kališ, 2008. Software: Blender 2.45)

Sledujme cestu libovolného prvku x (na obrázku prvky a, b, c) nosiče ***M*** grupy **G**. V první etapě cesty bijektivní zobrazení f přiřadí prvku vzájemně jednoznačně prvek $f(x)$ nosiče ***N*** grupy **H**, přičemž operace zůstanou zachovány. V druhé etapě cesty už putuje prvek x „převlečen" za prvek $f(x)$ do nosiče ***S*** grupy **S**. Bijektivní zobrazení g prvku $f(x)$ vzájemně jednoznačně přiřadí prvek $g(f(x))$ v nosiči ***S***, operace opět zůstanou zachovány. Pokud bychom zvolili $h = g(f(x))$, měli bychom požadované bijektivní zobrazení. Zbývá tedy už jen ověřit, zda-li zobrazení zachovává operace.

Zobrazení f a g jsou isomorfismy, tedy pro prvky a, b nosiče ***M*** grupy **G** a jejich obrazy v nosiči ***N*** grupy **H** platí:

$$f(aO_1b) = f(a)O_2f(b)\,, \qquad (6.a.1)$$

$$g(f(a)O_2f(b)) = g(f(a))O_3g(f(b)). \qquad (6.a.2)$$

My se tedy snažíme dokázat: $h(aO_1b) = h(a)O_3h(b)$.

Obraz prvku x v bijekci h jsme definovali jako složené zobrazení $g(f(x))$. Pokud toto aplikujeme na pravou stranu rovnosti, získáme $h(a)O_3h(b) = g(f(a))O_3g(f(b))$. Nyní využijeme rovností (6.a.2) a (6.a. 1), tedy

$$h(a)O_3h(b) = g(f(a))O_3g(f(b)) = g(f(a)O_2f(b)) = g(f(aO_1b)).$$

Nyní si stačí jen uvědomit, že prvek $g(f(aO_1b))$ je vlastně roven prvku $h(aO_1b)$. Tedy bijekce h

zachovává operace, je isomorfismem. Potom grupa **G** je isomorfní s grupou **S**, tedy isomorfismus grup je tranzitivní relace.

Dokázali jsme tedy, že můžeme každou grupu zařadit do určité třídy ekvivalence, kde jsou si všechny grupy až na isomorfismus rovny.

V předešlé kapitole jsme z hlediska isomorfismu rozdělili do skupin grupy cyklické. Každou skupinu jsme označili „významnou“ grupou, která ji reprezentovala. Následující věta nám řekne, že lze rozdělit do skupin všechny grupy, tj. nejen cyklické.

Věta (Cayleyho): Ke každé grupě **G** existuje grupa permutací $\mathbf{G}_p$, která je s **G** isomorfní.

◄ Důkaz (pouze nástin):

Věta nám říká dvě věci: Ke každé grupě **G** existuje grupa permutací. A že je tato grupa permutací isomorfní s grupou **G**. Pro platnost věty je třeba dokázat oboje. Nechť $\mathbf{G} = (\boldsymbol{M}, O, =)$ je libovolná grupa a prvek $a \in \mathbf{G}$.

1) Existence grupy permutací k libovolné grupě.

Mějme zobrazení a_p, které každému prvku x grupy **G** přiřadí prvek xOa grupy **G**. Tedy pokud je $a \in \mathbf{G}$, pak mu přiřadíme zobrazení

$$a_p: x \rightarrow xOa.$$

Jelikož a_p je bijektivní zobrazení a_p: $\boldsymbol{M} \rightarrow \boldsymbol{M}$, jedná se o permutaci množiny $\boldsymbol{M}$ podle definice permutace (viz kapitola Klasifikace grup). Budeme-li brát různé prvky a nosiče $\boldsymbol{M}$ grupy **G**, získáme vždy zobrazení a_p, což bude permutace množiny $\boldsymbol{M}$. Dá se dokázat, že množina permutací a_p všech prvků $a \in \mathbf{G}$, tvoří množinu všech permutací množiny $\boldsymbol{M}$. Tedy společně s operací „o_p“ skládání permutací a rovností „=“ permutací tvoří grupu permutací $\mathbf{G}_p = (\{a_p, a \in \mathbf{G}\}, o_p, =)$. Našli jsme tedy grupu permutací $\mathbf{G}_p$ k libovolné grupě **G**.

2) Isomorfismus grupy **G** s grupou permutací $\mathbf{G}_p$.

Mějme libovolnou grupu **G** a grupu permutací $\mathbf{G}_p$, která vznikla z prvků grupy **G** výše zmíněným způsobem. Zvolme zobrazení f: $\mathbf{G} \rightarrow \mathbf{G}_p$, které se řídí pravidlem $\forall a \in \mathbf{G}$; $a \rightarrow a_p$. Toto zobrazení přiřadí každému prvku nosiče grupy **G** prvek nosiče grupy permutací $\mathbf{G}_p$, respektive permutaci. Jelikož jsou permutace a_p odlišné, zobrazí se různé prvky grupy **G** na různé permutace grupy $\mathbf{G}_p$, zobrazení f je potom prosté. A jelikož je počet permutací a_p roven počtu prvků nosiče $\boldsymbol{M}$ grupy **G** (plyne z konstrukce zobrazení (permutace) a_p v předešlém kroku důkazu), je zobrazení f dokonce bijekce.

Podívejme se ještě, jakým způsobem zobrazení f přiřazuje dvěma prvkům grupy **G** jejich součin.

Nechť a, b jsou prvky nosiče grupy **G** a zobrazení f: $a \to a_p$ ($\forall\, a \in \mathbf{G}$), potom $f(a) = a_p$, $f(b) = b_p$ podle definice zobrazení f. Vypišme si nyní přehlednější zápis permutací a_p, b_p z $\mathbf{G}_p$ (pro x_1, x_2, ... z $\boldsymbol{M}$):

$$a_p = \begin{pmatrix} x_1 & , x_2 & , x_3 & ,\ldots \\ x_1 O a & , x_2 O a & , x_3 O a & ,\ldots \end{pmatrix}, b_p = \begin{pmatrix} x_1 & , x_2 & , x_3 & ,\ldots \\ x_1 O b & , x_2 O b & , x_3 O b & ,\ldots \end{pmatrix}.$$

Složením permutací $a_k\, o_p\, b_k = f(a) o_p f(b)$ pak získáme následující vztahy

$$x_1 \to x_1 O a \to (x_1 O a) O b,$$

$$x_2 \to x_2 O a \to (x_2 O a) O b,$$

$$x_3 \to x_3 O a \to (x_3 O a) O b,$$

... .

Jelikož je operace O grupy **G** asociativní, pro každý prvek x_k (kde $k \in \{1, 2, 3, 4, 5, ..., |\mathbf{G}|\}$) grupy **G** platí

$$x_k \to x_k O a \to ((x_k O a) O b = x_k O (a O b)).$$

Tedy vzniklá permutace $a_k\ o_p\ b_k$, přiřazuje každému prvku x grupy **G** prvek $xO(aOb)$,tuto permutaci můžeme potom zapsat jako

$$(aOb)_p: x \to xO(aOb).$$

Podle definice funkce f platí $(aOb)_p = f(aOb)$. Pokud se podíváme zpět a zhodnotíme výsledky našeho bádání, zjistíme, že jsme došli k rovnosti

$$f(a) o_p f(b) = f(aOb).$$

Tato rovnost společně s faktem, že zobrazení f je bijekce dokazuje, že existuje isomorfní zobrazení z libovolné grupy **G** do grupy permutací $\mathbf{G}_p$, tedy $\mathbf{G} \simeq \mathbf{G}_p$.►

Pozn. 1: Způsob, jakým jsme vytvořili permutace a_p, byl pomocí tzv. *pravostranného násobení*. Grupa permutací vytvořená tímto způsobem k účelu reprezentace dané grupy **G** se nazývá *pravostranná reprezentace*. Důkaz Cayleyho věty by se dal provést i zavedením permutací pomocí *levostranného násobení*, tedy pro nějaký prvek a grupy **G** vytvoříme permutaci a_p následovně

$$a_p: x \to aOx.$$

Důkaz věty by potom probíhal obdobně. Takovéto grupy permutací bychom pak nazvali *levostranné reprezentace*.

Pozn. 2: Část 1) důkazu Cayleyho věty v podstatě popisuje, jakým způsobem můžeme vytvářet prezentaci dané grupy grupou permutací.

Příklad 8.1.: Mějme grupu **H** = (***M*** = {*e*, *a*, *b*, *c*}, *O*, =), jejíž multiplikační tabulka je znázorněna tabulkou Tab. 8.1. Vytvořme pro **H** grupu permutací $\mathbf{H}_p$, která je s ní podle Cayleyho věty isomorfní.

Tab. 8.1. Multiplikační tabulka grupy **H** z příkladu 8.1.

O	*e*	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

Pro každý prvek množiny ***M*** vytvořme permutaci způsobem, popsaným v části 1) důkazu Cayleyho věty, tedy

e_p: $e \to (eOe = e)$, $a \to (eOa = a)$, $b \to (eOb = b)$, $c \to (eOc = c)$.

a_p: $e \to (aOe = a)$, $a \to (aOa = e)$, $b \to (aOb = c)$, $c \to (aOc = b)$.

b_p: $e \to (bOe = b)$, $a \to (bOa = c)$, $b \to (bOb = e)$, $c \to (bOc = a)$.

c_p: $e \to (cOe = c)$, $a \to (cOa = b)$, $b \to (cOb = a)$, $c \to (cOc = e)$.

Získáme tedy permutace $e_p = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$, $a_p = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}$, $b_p = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}$, $c_p = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}$, které tvoří nosič grupy permutací $\mathbf{H}_p$. Potom grupa $\mathbf{H}_p = (\{e_p, a_p, b_p, c_p\}, o_p, =)$ s operací o_p skládání permutací je (pravostrannou) reprezentací grupy **H**.

Pozn.: Grupy permutací byly v historii do hloubi prostudovány, proto se vyplatí při práci s nějakými speciálními grupami odvolávat na výsledky studií jejich reprezentací grupami permutací.

Reference: [**GOI**], [**KOT**], [**NII**].

9. Závěr

Teorie grup je velmi obsáhlá a barvitá. V diplomové práci se dotýkám pouze základních témat a nepouštím se do detailů. Mým přínosem je způsob pracování této diplomové práce. Snažil jsem se o přehlednost, systematičnost a vhodné zpracování textu pro cílovou skupinu studentů učitelství. Tuto práci jsem také zpracoval v interaktivní digitální formě, která se nachází na CD nosiči, připojeném k této diplomové práci. Mým cílem bylo vytvořit tento text také v podobě, která se podle mého názoru bude v budoucnosti vyskytovat zcela běžně, tedy především s možností interaktivního vyhledávání v textu pomocí hypertextových odkazů.

Teorie grup se dotýká spousty věcí našeho světa a samozřejmě i světa matematiky. V této kapitole bych ještě rád shrnul některé ukázky využití teorie grup.

Matematika

Využití teorie grup v matematice je značné především v důsledcích jejích stěžejních vět jako je věta Lagrangeova nebo Cayleyho. Pro připomenutí: Lagrangeova věta popisuje řády podgrup dané grupy. Cayleyho věta říká, že k libovolné grupě existuje grupa permutací, která je s původní grupou isomorfní. Pomocí nástroje isomorfismu vytváří teorie grup mosty mezi jednotlivými matematickými disciplínami. To, co se nedá vyřešit v teorii množin se dá za pomocí správné reprezentace například v grupě matic typu $n \times n$ řešit lépe. Pomocí teorie grup bylo dokázáno i mnoho domněnek z oblasti řešitelnosti určitých algebraických rovnic. Dále byly díky jejím výsledkům dokázány některé z domněnek řešitelnosti určitých typů konstrukčních úloh.

V polovině 17. století Pierre de Fermat bez důkazu formuloval jednu z nejznámějších vět, které se dnes říká Velká Fermatova věta. Ve skutečnosti zůstala po dlouhá léta pouze domněnkou, jelikož Fermat za celý svůj život k jejímu důkazu pouze podotkl, že je jednoduchý, ale už se mu nevejde na okraj stránky jeho výtisku Diofantovy Aritmetiky. Na jejím dokazování pohořeli i známí matematici jako Euler, Dirichlet nebo Cauchy. Ke zlomovému okamžiku došlo až v roce 1984 (po více než 300 letech), kdy byl důkaz Velké Fermatovy věty dán do souvislosti s důkazem tzv. Taniyama-Shimurovi domněnky, která se týkala eliptických křivek, což byla jiná oblast matematiky, která byla ve větší míře studovaná až v 19. a 20. století. Velká Fermatova věta byla dokázána až v roce 1994 A. Wilsonem, který mimo jiné použil teorii reprezentace grup a isomorfismu. V tomto případě by Wilson bez teorie grup neobstál. Pro zajímavost: Důkaz Fermatovy věty patří mezi nejdelší důkazy v dějinách matematiky – má včetně dodatků kolem 120 stran. Pokud má o něj čtenář zájem, je tento klenot matematické literatury k dispozici (bez dodatků) na internetových stránkách (pouze v angličtině): http://math.stanford.edu/~lekheng/flt/wiles-small.pdf.

Kryptografie

Kryptografie je vědní obor, zabývající se metodami utajování smyslu zprávy převodem do podoby, která je čitelná pouze se speciální znalostí. Tedy jinými slovy se jedná o šifrování. Historie šifrování spadá už do dob antiky, kdy vojenští generálové šifrovali zprávy z bojiště pomocí různých substitucí nebo znakových klíčů. V dnešní době je tento obor na mnohem vyšší úrovni. Šifruje se vše: Informace o bankovních převodech, data přenášená internetem, zdrojové kódy softwarových aplikací při kompilaci, přístupové kódy k domovnímu alarmu. Na světě jsou vždy lidé, kteří se zabývají prolomením těchto šifer. Proto je třeba vymýšlet stále nové, dokonalejší šifry a testovat současné. V současnosti se ve veliké míře využívá teorie čísel, především modulární aritmetiky, což jsou operace na grupě $\mathbb{Z}_n$ (pro konečné přirozené číslo *n*). Právě zde se využívá výsledků teorie grup, studiem struktur a vlastností znakových klíčů.

Umění

Vezmeme-li v úvahu symetrie daného rovinného útvaru a jejich skládání, můžeme v mnoha případech dojít k závěru, že daná struktura je grupa. Spousta moderních umělců se nechala inspirovat matematickými objekty a využila jich ve svých dílech. Grupy symetrií jsou jedny z nejhezčích matematikou inspirovaných uměleckých děl. Spoustu takových vzorů může čtenář najít na internetových stránkách uvedených níže, včetně mého oblíbeného M. C. Eschera, který patřil mezi přední světové umělce 20. století.

Odkazy na ukázky uměleckých děl inspirovaných grupami symetrií:

1) Některé japonské vzory (anglicky)

Dostupné z: <http://mathmuse.sci.ibaraki.ac.jp/pattrn/PatternE.html>.

2) Počítačem generované vzory Hanse Kuipera (anglicky)

Dostupné z: <http://web.inter.nl.net/hcc/Hans.Kuiper/17system.htm>.

3) Galerie M. C. Eschera (anglicky)

Dostupné z: <http://www.mcescher.com/>.

Seznam užitých pramenů

[**BAM**] Bartsch, Hans J.: *Matematické vzorce*. Třetí, revidované vydání. Mladá fronta. Praha, 2000. ISBN 80-204-0607-7.

[**BIA**] Bican, L.: Algebra (pro učitelské studium). 1. vydání. Academia. Nakladatelství Akademie věd České republiky. Praha, 2001. ISBN 80-200-0860-8.

[BJ1] Beachy, John A.: *Abstract Algebra: A Study Guide for Beginners*. [online]. Department of Mathematical Sciences. Northern Illinois University, 2006. [cit. dne 13.8. 2007]. Dostupné z: <http://www.math.niu.edu/~beachy/abstract_algebra/guide/contents.html>.

[**BJ2**] Beachy, John A.: *Abstract Algebra: Review Problems on Groups and Galois Theory*. [online]. Department of Mathematical Sciences. Northern Illinois University, 2006. [cit. dne 13.8. 2007]. Dostupné z: <http://www.math.niu.edu/~beachy/abstract_algebra/>.

[**COE**] Connell, Edwin H.: *Elements of Abstract and Linear Algebra*. [online]. Departments of Mathematics. University of Miami, 1999. [cit. Dne 13.8. 2007]. Dostupné z: <http://www.math.miami.edu/~ec/book/>.

[**GAI**] Gaglione, T.: *An Introduction to Group Theory*. [online]. [cit. Dne 13.8. 2007]. Dostupné z: <http://web.usna.navy.mil/~wdj/tonybook/gpthry/tonybook.html>.

[**GOI**] Goins, E. H.: *Abstract Algebra. Introduction to Group Theory*. [online]. California Institute of Technology, October 2002 – December 2002. [cit. dne 13.8. 2007]. Dostupné z: <http://homepage.mac.com/ehgoins/>.

[**GOA**] Goodman, Frederik M.: *Algebra: Abstract and Concrete*. [online] Edition 2.5. Semisimple Press. Iowa, 2006. [cit. dne 13.8. 2007]. Dostupné z: <http://www.math.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html>.

[**KOT**] Kopka, J.: *Teorie grup a dalších algebraických struktur*. 1. vydání. Univerzita J. E. Purkyně. Ústí nad Labem, 2001. ISBN 80-7044-367-7.

[**MIG**] Milne, J. S.: *Group Theory*. [online] v2.11. August 29, 2003. [cit. dne 13.8. 2007]. Dostupné z: <http://www.jmilne.org/math/CourseNotes/math594g.pdf>.

[**NII**] Niblo, Graham A.: *An Introduction to Group Theory*. [online]. August 13, 1999. [cit. dne 13.8. 2007]. Dostupné z: <http://www.maths.soton.ac.uk/~gan/MA203Notes1997.pdf>.

[**OCR**] O´Connor, J. J.; Robertson, E. F.: *The Development of Group Theory*. [online]. [cit. dne 4.5. 2008]. Dostupné z:

<http://www-history.mcs.st-andrews.ac.uk/HistTopics/Development_group_theory.html>.

[**VIV**] Vild, J.: *Visualisation of Small Groups*. Proc. of the 8th Internat. Conf. "Virtual University" (VU´07), SK, Bratislava, 13-14 December 2007, pp. 269-274. ISBN 978-80-89316-09-0.

[**WAI**] Waner, S.: *Introduction to Group Theory.* [online]. July 2003. [cit. dne 13.8. 2007]. Dostupné z: <http://www.zweigmedia.com/RealWorld/textindex.html>.

[**WEC**] Weisstein, E. W.: *Cycle Graph*. [online]. [cit. dne 3. 5. 2008]. Dostupné z: <http://mathworld.wolfram.com/CycleGraph.html>.

[**WIK**] *Group Theory.* [online]. Wikipedia, the free online encyclopedia. [cit. dne 13.8. 2007]. Dostupné z: <http://en.wikipedia.org/wiki/Group_theory>.